Marjo Valjakka

AMMATTIKORKEAKOULUN HENKILÖSTÖN TIEDONHALLINTAOSAAMISEN KEHITTÄMINEN

Opinnäytetyö
Sähköinen asiointi ja arkistointi

2017

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Marjo Valjakka	Tradenomi (YAMK)	Marraskuu 2017

Opinnäytetyön nimi

Ammattikorkeakoulun henkilöstön tiedonhallintaosaamisen kehittäminen

61 sivua
6 liitesivua

Toimeksiantaja

Laurea-ammattikorkeakoulu

Ohjaaja

Jukka Selin

Tiivistelmä

Digitalisaation myötä ammattikorkeakoulujen opetus- ja tukihenkilöstö tarvitsee yhä moninaisempia tieto- ja viestintätekniikan taitoja. Digiosaaminen on poisoppimista vanhoista toimintatavoista ja tiedon hyödyntämistä uusien tekniikoiden avulla. Digitaitojen ydin on kuitenkin asianmukainen tiedonhallinta. Henkilöstön on osattava toimia niin, että organisaation tieto on turvassa ja että tietoja käsitellään henkilöiden oikeuksia kunnioittaen. Paitsi että hyvän tiedonhallinnan toteuttaminen on ammattikorkeakouluille laissa säädetty velvollisuus, on se myös oleellinen osa hyvää palvelua, toiminnan turvaamista ja maineen hallintaa. Julkisina organisaatioina ammattikorkeakoulujen on myös näytettävä toteen, että sen palveluksessa olevilla on tarvittavat tiedot ja taidot henkilötietojen käsittelyyn, tiedon julkisuuteen ja salassapitoon, tietojen suojaamiseen sekä tietoturvallisuuteen liittyen.

Opinnäytetyössäni selvitin Laurea-ammattikorkeakoulun henkilöstön tiedonhallinnan osaamisen nykytilaa osaamistestin ja haastatteluiden avulla sekä pohjautuen omiin havaintoihini ammattikorkeakoulun työntekijänä. Selvityksen perusteella henkilöstöllä on jossain määrin puutteita kaikilla tiedonhallinnan osa-alueilla. Erityisesti nousivat esiin julkisen ja salassa pidettävän tiedon käsittely, tietoturvallinen viestintä sekä arkaluonteisen tiedon prosessit. Hyvää tiedonhallintaa ei ole otettu myöskään systemaattiseksi osaksi osaamisen johtamista.

Tavoitetilassa kaikilla laurealaisilla on esittämäni mukainen tiedonhallinnan perusosaaminen, joka pohjautuu lain ja asetusten vaatimuksiin sekä kansallisiin suosituksiin. Lisäksi esimiestehtävissä toimivat sekä luottamuksellista ja kriittistä tietoa käsittelevät henkilöt ovat täydentäneet osaamistaan vielä seuraavalle tasolle. Tavoitetilaan pääsemisen keinoja ovat osallistavat työmenetelmät, selkeä viestintä, johdonmukainen perehdyttäminen, vertaisohjaus sekä kohdennetut koulutukset. Tiedonhallinnan osaamista on myös mitattava säännöllisesti, jotta sitä voidaan kehittää myös tulevaisuuden tarpeita silmällä pitäen.

Asiasanat

Tiedonhallinta, tietosuoja, tietoturva, osaaminen

Author (authors)	Degree	Time
Marjo Valjakka	Master of Business Administration	November 2017
Thesis Title Developing employees' information management competence at an University of Applied Sciences		61 pages 6 pages of appendices
Commissioned by Laurea University of Applied Sciences		
Supervisor Jukka Selin		

Abstract

The need for the employees' diverse competence in information and communication technology at universities of applied sciences has increased along with digitalization. Digital knowledge consists of unlearning the old habits and utilizing the information with the help of the new technology. The core of digital knowledge is, however, information management competence. Employees have to know how to keep the information safe and handle the personal data by respecting the rights of the persons.

Information management is a legislated obligation for the universities of applied sciences but also an essential part of good service, securing the operations and management of reputation. Besides, universities of applied sciences have the obligation to indicate that the employees have the necessary knowledge of handling the personal, public and confidential data as well as protecting and securing the information.

In this thesis, I examined the present state of the information management competence of the employees at Laurea University of Applied Sciences with a knowledge test, interviews and based on my own observations as a staff member. Based on the study the employees had some lack of knowledge with all fields of the information management, specifically when handling the public and confidential information, using information secure communication and handling processes with sensitive data. In addition, information management was not a systematic part of competence management.

In the goal state, all the employees of Laurea would have achieved the basic level of information management competence, based on the requirements of the laws, regulations and national recommendations. Additionally, superiors and the employees handling confidential and sensitive information have reached the upper levels of knowledge. The means for accessing the goal state are collaborative working methods, clear communication, consistent orientation, peer guidance and targeted training. It is also essential to measure the quality of the information management competence regularly in order to develop the future needs.

Keywords

Information management, data protection, data security, competence

SISÄLLYS

1 JOHDANTO

Tieto on organisaatioiden elinehto ja tärkein voimavara. Samalla kun tiedon täytyy olla helposti hyödynnettävissä, on sen oltava myös suojeltu ja turvassa. Tätä kaikkea varten tarvitaan toimivaa tiedonhallintaa, joka käsittää koko tiedon elinkaaren hallinnan tietosisällön luomisesta sen organisointiin, käyttöön ja säilyttämiseen tai hävittämiseen asti. Julkisten organisaatioiden on julkisuuslain 18 §:n mukaan huolehdittava siitä, että sen palveluksessa olevilla on tarvittava tieto asiakirjojen julkisuudesta ja salassa pidosta, tietojen antamisesta ja luovuttamisesta, tietojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä sekä tietoturvallisuusjärjestelyistä ja tehtävänjaosta. Hyvän tiedonhallintavan mukaisesti organisaatioiden on myös pystyttävä varmistamaan, että määräyksiä ja ohjeita noudatetaan. Lisäksi toukokuussa 2018 alkaen sovellettava EU:n tietosuoja-asetus asettaa yhä enemmän vaatimuksia organisaatioiden henkilötietojen käsittelylle.

Samalla kun hallitus on vähentänyt määrärahoja korkeakouluilta, on hallitusohjelma asettanut myös vaatimuksia niiden digitalisaation edistämiselle. Uusien teknisten ratkaisuiden hyödyntämiseksi ja digitaalisten palveluiden kehittämiseksi on ammattikorkeakouluissa ymmärrettävä teknisen kehityksen mukanaan tuomat vaatimukset tietojen käsittelylle. Jotta ammattikorkeakoulut voivat toimia kolmella tehtäväalueellaan opetuksessa, tutkimus- ja kehitystyössä ja aluekehityksessä suunnannäyttäjinä, on henkilöstöllä oltava riittävät valmiudet myös digitaalisen tiedon hallintaan

Opinnäytetyöni toimeksiantaja on Uudellamaalla toimiva Laurea-ammattikorkeakoulu, jonka yhtenä strategisena osaamisalueena on henkilöstön digiosaamisen kehittäminen. Digiosaamisella ei ole kuitenkaan pohjaa, jos ei ymmärretä tiedonhallinnan perusteita. Uusissa digitaalisissa toimintamalleissa on osattava toimia tietoa turvaten, henkilöiden oikeuksia kunnioittaen ja tiedon saatavuutta edistäen.

Työssäni tutkin syksyn 2017 aikana henkilöstön tiedonhallintaosaamisen nykytilaa osaamistestin ja kahden avainhenkilön haastattelun avulla sekä pohjautuen omiin havaintoihini Laurea-ammattikorkeakoulun työntekijänä. Selvi-

tyksen tarve pohjautuu siihen, että Laureassa on herätty lainsäädännön ja toimintaympäristön asettamiin vaatimuksiin. Oletus on, että henkilöstön tiedonhallinnan osaamisen valmiudet vaihtelevat, eivätkä kaikki ole omaksuneet tietoturvaan ja- suojaan liittyviä vaatimuksia hyvän tiedonhallintatavan mukaisesti. Tavoitteenani on antaa eväitä hyvän tiedonhallintatavan takaamiseen vahvistamalla henkilöstön osaamista erityisesti tietosuojaan ja tietoturvaan liittyvissä asioissa. Tavoitetilan ja toimenpide-ehdotukset määrittelen opinnäytetyössäni lainsäädännön asettamiin vaatimuksiin, kansallisiin suosituksiin sekä aihepiiriin kuuluviin tutkimuksiin ja julkaisuihin pohjautuen.

Opinnäytetyön toisessa luvussa esittelen kehittämistehtäväni toteutuksen, asetan tutkimuskysymykset ja rajauksen sekä kuvaan aiempia aihepiiriin liittyneitä tutkimuksia. Seuraavassa luvussa käyn läpi tiedon ja tiedonhallinnan käsitteitä ja niitä ohjaavia vaatimuksia, jonka jälkeen syvennyn tarkemmin vielä tietoturvallisuuteen ja tietosuojaan. Viidennessä luvussa kuvaan ammattikorkeakoulun tiedonhallintatietämyksen nykytilaa kartoittamalla henkilöstön osaamistasoa sekä analysoimalla ammattikorkeakoulun nykyisiä ohjeita ja toimintaprosesseja. Luvussa kuusi asetan tavoitetilan, ja seitsemännessä luvussa kuvaan keinoja tavoitetilaan pääsemiseksi. Lopuksi pohdin, miten opinnäytetyöni on vastannut tutkimuskysymyksiini ja asetettuihin tavoitteisiin ja mitä asioita olisi syytä vielä tutkia aiheeseen liittyen.

2 OPINNÄYTETYÖN TOTEUTUS

Koska omaan yli kymmenen vuoden työkokemuksen ammattikorkeakoulun tukipalveluissa, voin sanoa tuntevani kohtalaisen hyvin tutkimukseni kohderyhmän, ammattikorkeakoulun henkilöstön. Tämä osaltaan myös selittää sen, miksi olen valinnut oman työyhteisöni tutkimuksen kohteeksi. Opinnäytetyöni aiheena on ammattikorkeakoulun henkilöstön tiedonhallinnan osaamisen kehittäminen. Tavoitteenani on Laurean tiedonhallinnan kokonaisvaltainen tarkastelu ja siihen liittyvän osaamisen kehittäminen tapaustutkimuksen näkökulmasta ja käytännön lähtökohdista. Tulkinta ja päätelmät muodostuvat kuitenkin vasta, kun olen ulkoistanut omat sisäiset ennakko-oletukseni aiheesta ja tulkinnut tulokset teoreettisen viitekehyksen avulla. Hermeneuttisen kehän

mukaisesti tarkoituksenani on näin ymmärtää kanssani samassa toimintaympäristössä toimivien henkilöiden käyttäjäkokemuksia ja kehittää tätä kautta yhteisiä tiedonhallinnan toiminta- ja ajattelutapoja. (Vilkka 2015, 100 - 112.)

2.1 Tutkimustavoitteet ja –menetelmät

Tapaustutkimuksen tutkittava kohde on Laurea-ammattikorkeakoulun henkilöstön tiedonhallintaosaaminen ja sen nykyinen hallintamalli. Opinnäytetyöni tavoitteena on luoda suunnitelma, jonka avulla jokainen ammattikorkeakoulun työntekijä pystyy ottamaan hyvän tiedonhallintatavan osaksi arkityötään. Työssäni keskityn hyvän tiedonhallinnan perusosaamiseen, joka koskettaa kaikkia henkilökunnan jäseniä. Tästä syystä olen rajannut pois henkilöryhmät, joiden osaamistarpeet on määriteltävä erikseen. Aihepiireinä nämä koskevat erityisesti kriittisiä tai arkaluonteisia tietoja sekä esimiestyön, henkilöstönhallinnon ja tutkimus-, kehitystyön erityiskysymyksiä.

Tutkimuskysymyksinä opinnäytetyössäni ovat

- Millä tavalla –Laurea-ammattikorkeakoulun nykyiset toimintamallit tukevat hyvän tiedonhallintatavan omaksumista?
- Miten Lauren henkilöstö on omaksunut erityisesti tietosuojaan ja tietoturvaan liittyvät kysymykset?
- Mihin asioihin on syytä kiinnittää erityistä huomiota, jotta henkilöstöllä on tarvittava tieto tietojen julkisuuteen, käsittelemiseen, suojaamiseen ja turvaamiseen liittyvistä menettelyistä ja että he toimivat ohjeiden mukaisesti?

Tutkimusmenetelminä olen käyttänyt monimetodisia lähestymistapoja, joissa olen yhdistänyt sekä laadullista että määrällistä tutkimusta. Tutkimusmateriaalina toimivat henkilöstölle tehdyn osaamisen kartoituksen testin tulokset sekä kaksi teemahaastattelua. Lisäksi olen havainnoinut toimintaa Laurean työntekijänä kartoittamalla Laureassa olemassa olevia ohjeita ja käytänteitä.

Henkilöstön osaamista olen mitannut henkilöstölle suunnatun osaamistestin avulla, johon 101 laurealaista vastasi henkilöstön kehittämispäivien yhteydessä elokuussa 2017. Vilkan (2015, 61) mukaan ennen kyselylomakkeen suunnittelua tulee kvantitatiivisessa tutkimuksessa olla päätettynä teoreettinen viitekehys ja keskeiset käsitteet, koska niihin liittyvien käsitteiden avulla voidaan mitata tutkittavaa asiaa. Käytännössä henkilöstön osaamista mittaava

kyselylomake oli tehty tietohallintotiimin yhteistyönä jo ennen opinnäytetyön aloittamista, joten osaamistestin tulokset ohjasivat ennemminkin opinnäytetyön tavoitteiden asentaa. Tämä ei mielestäni kuitenkaan haitannut teoreettisen viitekehyksen muodostumista. Osaamistestin tuloksia olen analysoinut työssäni soveltuvin osin.

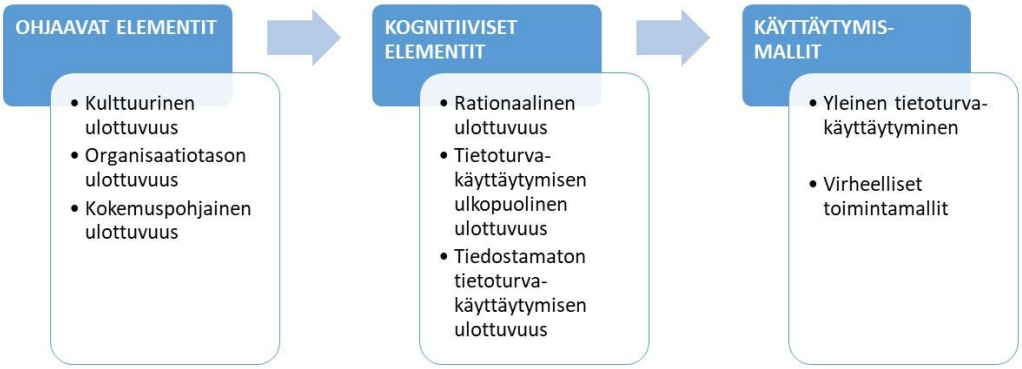
Osaamistesti ei kokonaisuudessaan vastannut tutkimuskysymyksiini, joten olen täydentänyt tutkimusaineistoa Laurean turvallisuusjohtajan ja henkilöstöjohtajan teemahaastatteluilla lokakuussa 2017. Haastateltavat valitsin heidän asiantuntemuksensa perusteella. Turvallisuusjohtajaa haastattelin puhelimitse ja henkilöstöjohtajaa kasvokkain noin tunnin ajan. Haastatteluissa pyrin kartoittamaan johtajien ajatuksia ja heidän haasteinaan pitämiään asioita henkilöstön tiedonhallintaan liittyen omien vastuualueidensa (kokonaisturvallisuus ja HR) näkökulmasta.

2.2 Aikaisempi tutkimus

Työni tueksi tutustuin aikaisempiin henkilöstön tiedonhallintaosaamiseen liittyviin tutkimuksiin, joita on tehty lähinnä tietoturvallisuuden ja siihen liittyvän koulutuksen näkökulmasta. Lisäksi sosiaali- ja terveysalan erityisluonteen vuoksi on tutkittu alan henkilöstön tietosuojaosaamista ja sen vaikutuksia toimintaan. Aiemmista tutkimuksista pyrin löytämään vastauksia henkilöstön osaamisen kehittämiseen ja hyvän tiedonhallintatavan varmistamiseen ammattikorkeakoulumaailmassa.

Kruger & Kearney (2006) ovat tutkineet sosiaalipsykologiaan perustuvaa menetelmää, jolla työntekijöiden tietoturvallisuuteen liittyviä asenteita, käyttäytymistä ja tietoa voitiin mitata kansainvälisessä kaivosyhtiössä. He toteavat, että henkilöstön piittaamattomuus tietoturvallisuudesta on yksi suurimmista riskeistä tietoturvallisuudelle ja että pelkkä tietoturvallisuusohjelman luominen ei lisää henkilöstön ymmärrystä siitä, mikä on heidän roolinsa tietoturvallisuuden takaamisessa. Käyttäjien tietoisuuden lisääminen ja riskien tunnistaminen vaativat jatkuvaa ja mitattavissa olevaa toimintaa. Tutkimuksen perusteella johto sai menetelmän avulla palautetta tietoturvallisuuden tasosta ja pystyi sitä kautta suuntaamaan strategisia kehittämiskohteita tietoturvallisuuden osa-alueisiin. (Kruger & Kearney 2006.)

Mari Karjalainen (2011) on luonut väitöstyössään metateorian tietoturvakoulutukselle. Myös hänen mukaansa työntekijät ovat yksi suurimmista uhkista organisaation tietoturvallisuudelle. Hän esittää, että tehokkaan koulutusmenetelmän lisäksi on tärkeää ymmärtää syitä työntekijöiden tietoturvakäyttäytymiselle. Tietoturvakoulutuksen pedagogiset vaatimukset hän määrittelee psykologisen, sisällöllisen, opetusmetodien ja oppimisen arvioinnin kontekstissa. Lisäksi hän on luonut teoreettisen viitekehyksen (kuva 1), joka auttaa ymmärtämään työntekijöiden tietoturvakäyttäytymisen syitä.



Kuva 1. Tietoturvakäyttäytymisen teoreettinen viitekehys (Karjalainen 2011).

Tietoturvakäyttäytymisen teoreettisen viitekehyksen ohjaavina elementteinä ovat kulttuurinen, organisaatiotason ja kokemuspohjainen ulottuvuus. Organisaatiotason ulottuvuudessa viestintä on Karjalaisen mukaan perusta tietoturvallisen käyttäytymisen edistämiselle, jotta työntekijät ymmärtävät tiedon arvon työssään. Viestintä pitää sisällään niin tietoturvapolitiikan, suullisen viestinnän, koulutukset kuin johdon roolin ja sitoutumisen. Se kattaa myös määräykset, valvonnan, palkkiot, rangaistukset ja pakkokeinot, joiden keinoja Karjalainen kuitenkin pitää työntekijöiden tietoturvakäyttäytymisen vaikuttamiseen kiistanalaisena. Viestinnän ja koulutuksellisen lähestymistavan suunnittelussa auttaa puolestaan kulttuurisen ulottuvuuden tunteminen, joka pitää sisällään organisaatiokulttuurin, yhteiskunnan normit sekä henkilön oman kulttuurisen taustan. Lisäksi on ymmärrettävä työntekijöiden käyttäytymistä kokemuspohjaisen ulottuvuuden kautta, joka kattaa heidän henkilökohtaiset ominaisuutensa ja aiemmat kokemuksensa esimerkiksi tietotekniikkaan liittyen.

Kaikilla näillä ohjaavilla tekijöillä on vaikutusta henkilön kognitiivisiin mekanismeihin. Yksi tärkeimmistä keinoista vähentää työntekijöiden epävarmoja toimintatapoja ja lisätä positiivisia muutoksia on rationaalinen ulottuvuus. Tutkimus osoittaa esimerkiksi, että hankalaksi koetuilla toimintatavoilla ja järjestelmillä voi olla merkittäviä vaikutuksia työntekijöiden tietoturvalliseen käyttäytymiseen. Kiinnittäessä ohjauksessa ja neuvonnassa tähän huomiota saadaan kuitenkin vähennettyä kokemusta järjestelmien vaikeudesta. On myös näytettävä järkiperusteisesti toteen, että ohjeiden noudattamatta jättämisellä on negatiivisia seurauksia, kun taas oikeat toimintatavat hyödyttävät omaa työtä. Lisäksi on ymmärrettävä, että henkilö ei useinkaan tee päätöstä noudattaa tai olla noudattamatta tietoturvallisuusohjeistuksia, vaan ne ovat osa henkilön tietoturvakäyttäytymisen ulkopuolista käyttäytymistä. Toimintatapoja noudatetaan, koska koetaan, että niin vain pitää tehdä ja koska toisetkin noudattavat niitä. Tiedostamattomaan ulottuvuuteen liittyvät puolestaan muun muassa inhimilliset virheet toimintatavoissa, jotka lisääntyvät työpaineen alla.

Käyttäytymismallit, jotka voivat olla vääriä toimintatapoja ja ohjeiden noudattamista tai noudattamatta jättämistä riippuvat kaikista edellä mainituista syistä ja niiden yhdistelmistä. Karjalainen toteaa, että tietoturvakoulutuksissa ja -ohjeistuksissa olisi hyvä ymmärtää niiden painoarvo ihmisen käyttäytymiselle ja korostaa sen johdosta eri perusteluita eri tarkoituksiin ja eri kohderyhmille. (Karjalainen 2011.)

Mäkinen (2013) on puolestaan tutkinut asiakirjahallintaa mobiilissa työssä. Hänen mukaansa asiakirjahallinto perustuu usein siihen oletukseen, että työtä tehdään toimistolla ja yhä yleistyvä mobiili tiedonhallinta nähdään teknisenä asiana, ei niinkään tiedonhallinnan työvälineenä. Kun tiedot ovat asiakirjahallinnon määräämissä paikoissa, on asiakirjahallinnon ammattilaisten helpompi hallita omaa työtään, joten he pyrkivät luomaan ohjeistukset ja käytännöt asianhallintajärjestelmiin pohjautuen. Työntekijät kuitenkin kokevat järjestelmät kömpelöinä ja vaikeasti saavutettavina. Asiakirjahallinto ei näin ole käyttäjäkeskeistä eikä tue mobiilia tiedonhallintaa, jolloin tieto hajautuu yhä useampaan paikkaan. Työntekijöille pääasia on vain, että heidän tarvitsemansa tieto on heillä itsellään käytettävissä. Ongelmana organisaatioille on kuitenkin se, että itse tuotettu asiakirja tai muu tieto nähdään usein omana eikä sitä jaeta tai koeta organisaation omaisuudeksi. Tuolloin tieto jää henkilön itse parhaaksi

kokemiin paikkoihin ja kun tietoa ei enää tarvita, ajatellaan että sen säilytys on jonkun toisen vastuulla. Mäkisen mukaan tiedonhallinnan käytäntöihin sitoudutaan, mikäli koetaan, että ne tukevat omia työtehtäviä. Yhdessä luodut ja organisaation ydintoimintoihin kytkeytyvät säännöt esimerkiksi tiedon säilyttämiselle ja käsittelylle toimivat paremmin kuin oman toiminnon ulkopuolelta tulevan yksikön määräämät ohjeet. (Mäkinen 2013.)

Sosiaali- ja terveysalan haasteena ovat erityisesti arkaluonteisten ja salassa pidettävien tietojen käsittely ja tietosuojariskien kasvumahdollisuudet. Jokelainen (2011) tutki Pro gradu –tutkielmassaan Kainuun maakunta –kuntayhtymän hoitohenkilöstön tietoturva- ja tietosuojatietämystä. Jokelaisen mukaan tietoturvapolitiikan, tietoturvallisuustavoitteiden ja potilastietojen lainmukaisen käsittelyn periaatteiden olemassaolo ei yksinään takaa hyvää tiedonhallintaa. Tutkielman perusteella Jokelainen ehdottaa, että organisaation on arvioitava henkilöstön nykytilan osaamista, määriteltävä toiminnan kannalta keskeinen tietoturvallisuuden ja tietosuojan osaaminen ja näiden pohjalta kehitettävä osaamistasoa. Osaamiskartoituksen pohjalta voidaan laatia ja toteuttaa tietosuoja- ja tietoturvaosaamisen kehittämissuunnitelma koko organisaatiotasolla. Riittävän ja kriittisen tietoturva- ja tietosuojaosaamisen määrittely voi kuitenkin olla haasteellista, sillä on pystyttävä ennakoimaan myös tulevaisuuden osaamistarpeita riittävän ajoissa. (Mt.)

Osaamista voidaan pitää yllä sitouttamalla henkilöstö organisaatioissa järjestettäviin koulutuksiin ja tiedottamalla muutoksista. Jokelainen myös ehdottaa, että tietosuojaan ja tietoturvaan liittyvä koulutus ja erilaiset tietopaketit kuuluisivat pakollisena osana uusien työntekijöiden perehdyttämistä. Käyttämällä organisaation osaamiskartoituksen tuloksia koulutusten oheismateriaalina ja sisällön suunnittelun apuna voidaan kohdentaa päähuomio todettuihin puutteellisuuksiin ja saada tietosuoja- ja tietoturvaosaaminen organisaation yhteiseksi asiaksi. Koulutuksissa on painotettava hänen mukaansa perinteisen teknisen osaamisen lisäksi yhä vahvemmin myös tietoturva-asenteita ja yksityisyyden varmistamista. (Mt.)

Yhteenvetona aikaisemmat tutkimukset osoittavat, että niin dokumenttien hallintaan, tietoturvallisuuden edistämiseen kuin koko organisaation tiedonhallin-

nan kehittämiseen on osallistettava koko henkilöstö tiedon käsittelijöistä raportointia hyödyntävään johtoportaaseen. Tämä vaatii koulutusta, sitouttamista ja ennen kaikkea keskustelevaa otetta yhteisen ymmärryksen ja hyödyn takaamiseksi. Kun ymmärretään se, miten organisaation toimintamallit ja työntekijöiden ominaisuudet vaikuttavat tiedonhallinnan osaamisen kertymiseen, voidaan vaikuttaa kertyvän tiedon lisäksi myös työntekijöiden motivaatioon ja asenteeseen tietosuojaa ja tietoturvaa kohtaan.

3 TIETO JA SEN HALLINTA

Tieto on yhä merkittävämpää yhteiskäyttöistä pääomaa, jonka arvo ja vaikuttavuus kasvavat jaettaessa. Ammattikorkeakoulun julkisin varoin kerättyä tietoa on käytettävä kustannustehokkaasti niin päätöksenteossa, opiskelijoille tuotetuissa palveluissa kuin toiminnan prosesseissa. Samalla julkisten tietojen tulee olla saatavilla ja salassa pidettävä tieto suojattuna ja turvattuna. Tämä kaikki edellyttää luotettavia ja yhteen toimivia tietoja, kokonaisvaltaista ja osaavaa tietojohtamista sekä laadukasta ja tehokasta tiedonhallintaa. Tiedonhallinnan tavoitteena on mahdollistaa tietojen löytäminen, käsittely ja hyödyntäminen koko tietojen elinkaaren ajan. (Valtiovarainministeriö 2017a.)

3.1 Tieto

Tiedon arvoketju on informaatiotutkimuksessa perinteisesti luokiteltu dataan, informaatioon, tietämykseen, ja viisauteen. Niistä data on merkeistä ja symboleista koostuvaa informaatiota, joka lopulta jalostuu inhimilliseksi viisaudeksi (Arkistolaitoksen arkistowiki 2013). Tieto voidaan myös jakaa tiedonhallinnan osa-alueittain asiakirjalliseen tietoon, ydintietoon, avoimeen tietoon, metatietoon sekä prosesseissa ohjautuvaan tietoon (JUHTA 2015). Työssäni haluan nostaa esille myös henkilötiedot, jotka sivuavat näitä kaikkia, ja joiden arvo on noussut digitaalisessa maailmassa yhä korkeammalle. Käyn seuraavassa vielä tarkemmin tiedon osa-alueita, ja pyrin löytämään niihin yhteyden myös ammattikorkeakoulujen näkökulmasta.

Asiakirjallinen tieto

Asiakirjallista tietoa on nykyisin noin 20-25 % organisaatioiden tiedosta (Aholainen 2017). Ne dokumentoivat organisaation tehtäviä ja siten takaavat toiminnan jatkuvuuden, jäljitettävyyden ja todistusvoiman. Asiakirjallisen tiedon vaatimuksista on määritelty sekä lainsäädännössä että arkistolaitoksen määräyksissä. Ammattikorkeakoulujen on siten esimerkiksi pidettävä yllä arkistonmuodostussuunnitelmaa, jolla hallitaan lähinnä paperisten asiakirjojen elinkaarta. Tavoite on kuitenkin yhä enenevissä määrin pyrkiä kohti sähköistä asiakirjahallintaa.

Ydintieto

Ydintiedot ovat organisaation keskeisintä ja pysyväisluonteista dataa, jota useampi prosessi tai toiminto tarvitsee samanmuotoisena. Ammattikorkeakoulujen ydintietoina voidaan pitää erityisesti opiskelija- ja henkilöstötietojen tietokantoja sekä talous- ja suorituslukuja, joiden ympärille koko ammattikorkeakoulujen toiminta keskittyy.

Avoin tieto

Avoin tieto on julkisesti saatavilla olevaa tietoa, jota voi koneluettavassa muodossa ottaa käyttöön maksutta ja avoimin käyttöehdoin. Sitä voidaan hyödyntää eri tarkoituksiin ja sovelluksiin. Ammattikorkeakouluissa avoimen tiedon tarve ja siihen liittyvät kysymykset erityisesti tutkimus- ja kehitystyössä ovat nousseet yhä vahvemmin esille viime vuosina ja sitä edistetään myös valtakunnallisena korkeakouluyhteistyönä.

Metatieto

Tiedon identiteettiä kuvataan asiasanoilla, joita kutsutaan metatiedoiksi. Metatietoa käytetään muun muassa tietojen haussa, tallentamisessa, yhdistämisessä sekä erilaisten työnkulkujen ohjauksessa. Tarkat metatiedot ovat edellytys tietojen semanttiselle yhteen toimivuudelle ja tehokkaalle hyödyntämiselle. Korkeakoulujen yhteydessä on tehty yhteistyötä muun muassa Opetus- ja kulttuuriministeriön RAKETTI-hankkeen tietovarasto-osiossa, jossa on määritelty korkeakoululaitoksen yhteisiä käsitteitä (Korkeakoulujen KA-pilottiryhmä 2013). Tämä edistää muun muassa erilaisten opintohallinnollisten tehtävien yhteen toimivuutta.

Prosesseissa ohjautuva tieto

Prosessien tiedonohjaus mahdollistaa automaattisen metatietojen määräytymisen ja asiakirjatietojen käsittelyn tietojärjestelmässä. Tiedonohjaus pohjautuu tiedonohjaussuunnitelmaan, joka on tietojärjestelmien taustalle laadittava metatietomääritys organisaation tehtävistä, käsittelyvaiheista ja asiakirjatyypeistä. (JUHTA 2016.) Tällä hetkellä tiedonohjaussuunnitelmatyö on käynnissä tai käynnistymässä useassa ammattikorkeakoulussa. Sen tavoitteena tukea sähköistä tiedonkulkua ja käsittelyprosesseja ja tätä kautta parempia sähköisiä palveluita.

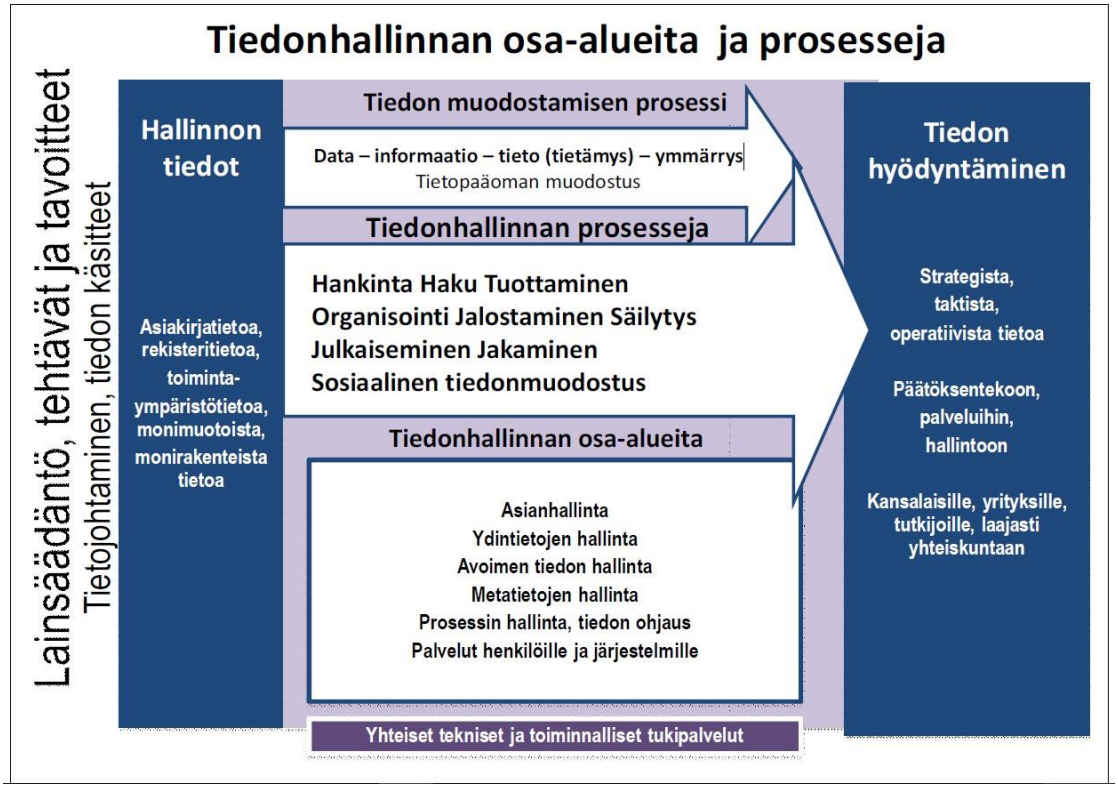
Henkilötieto

Henkilötietoja ovat kaikki luonnolliseen henkilöön liittyvät tiedot, jotka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen tai jonkin hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Henkilötietojen käsittelylle on aina oltava laissa säädetty käsittelyn oikeusperuste. Samaan käyttötarkoitukseen kerätyistä henkilötiedoista koostuvaan henkilörekisteriin kuuluvat kaikki ne tiedot, joita käytetään samassa käyttöyhteydessä riippumatta siitä, miten ja mihin ne on talletettu. (Tietosuojavaltuutetun toimisto 2010.) Arkaluonteisia henkilötietoja ovat tiedot, jotka kuvaavat henkilön rotua tai etnistä alkuperää, yhteiskunnallista, poliittista tai uskonnollista vakaumusta, ammattiliittoon kuulumista, rikollista tekoa tai sen seuraamusta, terveydentilaa, vammaisuutta ja niihin kohdistuvia toimenpiteitä sekä henkilön sosiaalihuollon tukitoimia. Arkaluonteisten tietojen käsittely on henkilötietolaissa asetetuin poikkeuksin kielletty. Ammattikorkeakoulujen keskeisimpiä henkilötietoja ovat opintohallinnon, henkilöstön ja sidosryhmien henkilörekistereissä olevat tiedot. Arkaluonteisten tietojen käsittelystä on määritelty erikseen ammattikorkeakoululain 40 §:ssä (Ammattikorkeakoululaki 2014).

3.2 Tiedonhallinta

Tiedonhallinta-käsitettä on määritelty niin lainsäädännössä kuin viranomaisten tuottamassa informaatiossa. Julkisen hallinnon tietoarkkitehtuurin mukaisesti tiedonhallinta kytkeytyy tietopääoman muodostamiseen, tiedonhallinnan prosesseihin sekä tiedonhallinnan osa-alueiden hallintaan, jotka kaikki tähtäävät

tiedon hyödyntämiseen päätöksenteossa, palveluissa ja hallinnossa. Tiedonhallinnan osa-alueet ja prosessit on koottu kuvaan 2.



Kuva 2. Tiedonhallinnan osa-alueita ja prosesseja (Valtiovarainministeriö 2017a).

Tiedonhallinnan tehtäviksi Voutilainen (2014) listaa käsiteltävien ja säilytettävien tietojen arvon, elinkaaren, säilytysmuodon, suojaustason ja käyttöoikeuksien määrittelyn. Yhtä tärkeää on myös huolehtia julkisuuteen, salassapitoon, tietosuojaan ja tietoturvaan liittyvistä vaatimuksista sekä hoitaa organisaation toimintaan liittyvää tietopalvelua. (Mt.)

Julkisen hallinnon neuvottelukunta (JUHTA 2015) on määritellyt tiedonhallintaa ohjaaviksi periaatteiksi julkisten tietojen saatavuuden ja uudelleen käytön mahdollistamisen, tietojen käytettävyyden, eheyden, luotettavuuden ja laadun varmistamisen koko tiedon elinkaaren ajan sekä tietosuojan, tietoturvan ja tietojen yhteen toimivuuden. Näitä periaatteita pyritään edistämään myös julkisen hallinnon digitaalisen turvallisuuden johtoryhmän VAHTI-ohjeilla. Oleellista on ymmärrys siitä, että tiedonhallinta ei ole vain organisaation yksittäinen tukitoiminto, vaan se on merkittävä osa tehtävien hoitoa, johtamista ja toiminnan tehokkuuden toteuttamista (Valtiovarainministeriö 2017b).

3.3 Tiedonhallinnan haastavat vastuut

Organisaatioiden tiedonhallinnan haasteina ovat Henttosen (2015, 198 - 199) mukaan tiedon saaminen oikealle henkilölle, käyttöoikeuksien hallinta ja metatietojen puutteellisuus. Linden (2015) puolestaan toteaa, että tiedon hallinnan ongelmia tuottavat tiedon saamisen viiveet, sisällön virheellisyys, tiedon ajantasaisuuden heikkous, sen piiloutuminen tai turvattomat käyttöoikeudet. Organisaatioissa ei tiedetä keneen ottaa yhteyttä, koulutus on puutteellista ja mahdolliset ohjeet ovat vanhentuneet, koska niiden päivitystä ei ole vastuutettu kenellekään. Yhteisenä tekijänä moniin ongelmiin voikin pitää vastuiden puutetta Ongelmat kertautuvat siten virheellisissä ja jopa haitallisissa toimintamalleissa ja hankaliksi koetuissa prosesseissa.

Hakkarainen-Kiri (2014) toteaa, että organisaatioissa ei useinkaan ole yksikköjä tai vastuutahoja, joille tiedon kokonaiskuva kuuluisi. Pääsääntöisesti tiedonhallinnasta vastaavat asiakirjahallinto tai tietohallinto. Voutilainen (2014) kiteyttää asiakirjahallinnon tehtäväksi tiedonhallinnan sisällöllisen määrittelyn ja laadunvalvonnan. Tietohallinnon tehtävänä on puolestaan luoda edellytykset ja välineet organisaation tiedonhallinnalle. Asiakirjahallintoa on kuitenkin arvosteltu takertumisesta katoaviin toimintamalleihin, jolloin asiakirjojen hallinta koetaan usein haasteelliseksi. Usein tavoitteena on, että asiakirjoja tallennetaan organisaation valvomaan asiakirjajärjestelmään, jonka keskitettyä luokitusta ja asiasanoitusta asiakirjahallinnon ammattilainen pitää yllä. Asiakirjajärjestelmistä ei kuitenkaan ole tullut sellaista ratkaisua, kuin mitä vielä 2000-luvun alussa toivottiin. Syinä voidaan pitää sitä, että käyttäjät toimivat ohjeistuksista huolimatta asiakirjajärjestelmien ulkopuolella ja että asiakirjahallinto kohdistaa huomionsa vain muutamaan prosenttiin kaikista aineistoista. Järjestelmiin saadaan talteen siis vain pieni osa aineistosta, ja tietoa on yhä edelleen pilvipalveluissa, verkkolevyillä, sähköpostiviesteissä ja muissa järjestelmissä. (Henttonen, 2015, 208.) Kun työntekijät tallentavat asiakirjoja henkilökohtaisiin tallennuspaikkoihinsa kuten tietokoneen työpöydälle ja sähköposteihin, yrityksellä ole juurikaan mahdollisuutta seurata syntynyttä tietosisältöä (Linden 2015).

Henkilötietojen osalta organisaatioille rekisterinpitäjänä kohdistuu vielä erityisiä vastuita, jotka liittyvät henkilötietojen suojaamiseen. Henkilörekisterien

omistajan lopullinen vastuu on aina organisaation johdolla, jonka täytyy huolehtia siitä, että henkilötietojen käsittelyyn liittyvät vastuut ja tehtävät on määritelty asianmukaiseksi. Henkilötietojen käsittely kattaa kaikki prosessit, joissa tietoa on suojattava ja turvattava. Toiminnan jatkuvuuden kannalta tiedonhallinta on myös oleellinen osa kokonaisturvallisuutta ja turvallisuusjohtamista, jonka vuoksi organisaatioissa tarvitaan yhteinen näkemys siitä, kuka on vastuussa tiedosta ja sen suojaamisesta.

Ammattikorkeakoulujen osalta tiedon osa-alueiden vastuut voi kuvata seuraavasti:

Asiakirjallisen tiedon hallinta

Asiakirjojen ja dokumenttien hallinta on olennainen osa ammattikorkeakoulujen prosessien toimivuutta. Paitsi että pelisäännöt niin sopimusten hallintaan kuin opiskelijoita koskevien asiakirjojen säilytysaikoihin ja -tapoihin sujuvoittavat työskentelyä, käytetään asiakirjallista tietoa myös päätöksenteon tukena erilaisten raporttien ja muistioiden muodossa. Lisäksi asiakirjat toimivat muistijälkenä ja todisteena toiminnasta myöhempää tarvetta varten. Ammattikorkeakouluissa asiakirjallisen tiedon hallinnasta ja ohjeistamisesta vastaavat yleensä asiakirjahallinnon ammattilaiset, joita ovat esimerkiksi arkistossa, kirjaamossa tai tietopalveluissa toimivat henkilöt. Varsinainen vastuu yksittäisen asiakirjan hallinnasta on kuitenkin aina asiakirjan tuottaneella henkilöllä.

Ydintietojen hallinta

Vilminko-Heikkisen (2016) mukaan ydintietojen kohdalla suurin vastuu pitäisi olla liiketoiminnasta vastaavalla taholla, koska ydintieto muodostaa rahanarvoisen perustan organisaation toiminnoille. Keskeistä ydintietojen hallinnassa on kunkin tiedon omistajuus. Ammattikorkeakouluissa ydintietojen vastuut kohdistuvat näin ydinprosesseista, kuten koulutuksesta ja tutkimus- ja kehitystyöstä vastaaviin tahoihin.

Metatietojen hallinta

Metatiedot kytkeytyvät vahvasti tietoarkkitehtuuriin, joka kuvaa organisaation tiedot ja niiden hyödyntämisen rakenteen ja sisällön. Se tukee tärkeimpien tietojen saatavuutta, käytettävyyttä ja yhteen toimivuutta, ja sitä edistetään muun

muassa julkisen hallinnon yhteisillä sanastoilla, koodistoilla ja rakennekuvauksilla. (JUHTA 2015.) Tietoarkkitehtuurityö on ammattikorkeakouluissa yleisesti tietohallintoyksikön alaista toimintaa, mutta sillä on vahva kytkös myös laatutoimintaan ja tiedonohjaukseen.

Avoimen tiedon hallinta

Avointa tietoa edeltää ammattikorkeakouluissa erityisesti tutkimus- ja kehittämistoiminnan aineistohallintasuunnitelma, jonka avulla selvitetään aineiston keräämisen ja käsittelyn tavat, tietosuojaan liittyvät kysymykset sekä aineiston mahdolliset avaamisen tavat. Avoimen tiedon koordinoinnin vastuut on yleensä jaettu kirjasto- ja tietopalveluiden sekä TKI-toiminnan kesken. On kuitenkin tärkeää, että myös asiakirjahallinto ja tietohallinto tukevat avoimen tiedon mahdollistamista omilla osaamisalueidensa puitteissa.

Prosesseissa ohjautuva tieto

Prosesseissa kulkevan tiedon hallinta on kiinteä osa asiakirjoihin pohjautuvaa tiedonohjaussuunnitelmatyötä, ja se pitää sisällään tiedon eri käyttötarkoitusten määrittelyn, tietojen luokittelun sekä tietoa tuottavien prosessien kuvaamisen tiedon elinkaaren eri vaiheissa. Ammattikorkeakouluissa tietosuunnittelusta vastaavat yleensä asiakirjahallinto ja tietopalvelut. Prosesseissa liikkuva tieto kytkeytyy kuitenkin tiiviisti myös laatutyöhön, jota toteutetaan prosessien omistajien kanssa ja joilla on konkreettinen vastuu tiedon ajantasaisuudesta.

Henkilötietojen hallinta

Henkilötietoja voi kuulua jokaiseen tiedon osa-alueeseen, joten niiden käsittelyä ei ole tietoarkkitehtuurissa erikseen luokiteltu omaksi tiedonhallinnan osa-alueekseen. Henkilötietojen hallinta on kuitenkin digitaalisessa ympäristössä entistä kriittisempää. Henkilötietojen hallinnasta vastaa rekisterinpitäjä, jonka käyttöä varten henkilörekisteri on perustettu ja jolla on oikeus määrätä henkilörekisterin käytöstä. Ammattikorkeakoulu on omien henkilörekistereidensä rekisterinpitäjä ja on vastuussa käsiteltävistä henkilötiedoista. Käytännössä henkilörekisterin asianmukainen käyttö on kuitenkin selkeästi määriteltävä ammattikorkeakoulun kyseisestä toiminnosta vastaavalle henkilökunnan jäsenelle, joka edustaa rekisterinpitäjää ja jonka yhteystiedot on myös ilmoitettava rekisteriselosteessa. (Karppinen & Johansson 2017.)

Tiedonhallinnan vastuut leikkaavat toisiaan läpi organisaation ja esimerkiksi tietohallinnon vastuulla olevan tietoarkkitehtuurin ja asiakirjahallinnon ylläpitämän tiedonohjaussuunnitelmatyön tehtävät ovat lähestymässä toisiaan. Tiedon ohjaukseen liittyvät tavoitteet voivat olla kuitenkin teknisesti suuntautuneille kokonaisarkkitehdeille vaikea sisäistää ja toisaalta asiakirjahallinnon ammattilaisten voi olla vaikea ymmärtää tietoarkkitehtuurin teknisiä termejä. Oppia ja yhteisen ymmärryksen jakamista tarvitaankin molemmin puolin. (Hakkarainen-Kiri, 47-48.) Tämän lisäksi niin henkilötietojen käsittelyssä, tietoarkkitehtuurityössä kuin asiakirjalliseen tietoon pohjautuvassa tietosuunnittelussa tarvitaan yhteistyötä ja yhteistä ymmärrystä myös prosessien omistajien ja johdon kesken. Lopullinen vastuu tiedon omistajuudesta on aina ammattikorkeakoulun johdolla. Tiedonhallinnan vastuut on siis hyvä määrittää johtoryhmätasolla, jotta päätökset saadaan jalkautettua myös arjen toimintoihin.

3.4 Tiedonhallintaosaaminen osana johtamista

Tiedolla johtaminen perustuu oikeaan ja reaaliaikaiseen tietoon. Tiedonhallinnan kytkeminen osaksi organisaation johtamista on kuitenkin yksi organisaation toiminnan merkittävistä haasteista. Johdolla on oltava kokonaiskuva toiminnan tarvitsemista tiedoista sekä niiden välisistä suhteista, jotta se pystyy tekemään päätöksiä oikeisiin tietoihin pohjautuen. Mitä enemmän laadukasta dataa on käytettävissä, sitä parempia tuloksia tietoja korreloimalla pystytään tekemään. Johdon on tämän vuoksi luotettava tiedon osa-alueiden asiantuntijoihin ja annettava resursseja tiedonhallinnan ylläpitoon ja kehittämiseen. (Jokelainen 2011.)

Johdon on myös pystyttävä käsittelemään tietoa kaikissa tilanteissa lain ja asetusten puitteissa. Tietoturvallisuuden ja yksityisyyden merkityksen lisääntyminen ovat lisänneet tarvetta johdon tietoturva-asenteiden sekä yksityisyydensuojan toteutumisen varmistamiseen. Jotta organisaatio voi osoittaa toteuttavansa tiedonhallintaa lain ja asetusten mukaisesti on sen oltava tietoinen organisaation tietosuojan ja tietoturvan nykytilasta ja mahdollisista tietoturvallisuusriskeistä voidakseen arvioida tarvittavat toimenpiteet tavoitteiden saavuttamiseksi. (Voutilainen 2012, 31-32.)

Koska julkisen hallinnon tietojohtaminen on varsin sääntelykeskeistä, korostuu tietojohtamisvalmiuksissa yhä enemmän myös informaatio-oikeudellisten perusteiden tunteminen. Niitä ovat tietoon liittyvät toimenpiteet ja oikeudet, kuten tiedon hankinta, käyttö, edelleen luovuttaminen, säilyttäminen ja hävittäminen. (Mt.) Koska esimiehet tekevät henkilötietojen käsittelyä koskevia päätöksiä, on heidän ymmärrettävä oma roolinsa henkilötietojen suojaan liittyen. Käytännössä johdon on ymmärrettävä omaan asemaansa liittyvän tietosuojan perusteet sekä vastuut, jotta se voi toimia esimerkkinä, ohjeistaa alaisia ja toisaalta varmistaa myös alaistensa oikeuksien ja velvollisuuksien toteutumisen. Konkreettisina toimenpiteinä johdon on organisoitava tiedonhallintatyö, hyödynnettävä tietosuojavastaavaa ja tietosuoja-/tietoturvaohjausryhmää ja varmistettava niin oma kuin koko henkilöstön tietoturva- ja tietosuojaosaaminen. (Andreasson ym. 2017.) Johdon on myös ymmärrettävä eri henkilötietoja käsittelevien tehtävänkuvien erilaiset osaamisvaatimukset tiedon käsittelyyn koko sen elinkaaren ajan.

Johdon on myös otettava huomioon, että uusilla digitaalisilla toimintamalleilla on vaikutusta paitsi tiedonhallintataitoihin myös koko työyhteisön toimintaan. Tämä vaatii erityisesti muutosjohtamisen ja osaamisen johtamisen taitoja. Osaamisen johtamisen avulla vahvistetaan organisaatiota, jossa työyhteisön jäsenet kehittävät yhdessä toimintaansa ja oppimishaasteitaan sekä luovat näin yhdessä uusia käytäntöjä (Juholin 2008, 175). Tällä kaikella on tärkeä merkitys myös organisaation maineen hallinnalle. Ongelmat henkilöstön tiedonhallintataidoissa saattavat hetkessä näkyä ulospäin.

3.5 Lainsäädäntö ja muut ohjaavat periaatteet

Ammattikorkeakoulut ovat osa julkista hallintoa, jonka tiedonhallintaa säädellään vahvasti lukuisilla eri lailla. Tietosuojaa ohjataan erityisesti lainsäädännön kautta, kun taas tietoturvaa toteutetaan myös erilaisten standardien avulla. Kuvaan seuraavassa keskeisimmän tiedonhallintaa ohjaavan sääntelyn.

Perustuslain 12.2 §:n mukaan viranomaisen hallussa olevat asiakirjat ovat julkisia, jollei niiden julkisuutta ole lailla erikseen rajoitettu. Julkisuusperiaatteen

tarkoituksena on mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, lisätä kansalaisten luottamusta viranomaisten toimintaan sekä saada tietoa viranomaisten toiminnasta. (Voutilainen 2012, 70-71.)

Laki viranomaisen toiminnan julkisuudesta eli julkisuuslaki on viranomaistoiminnan julkisuus- ja salassapitolainsäädännön keskeisin säännös. Se tarkentaa perustuslaissa säädetyn julkisuusperiaatteen toteuttamista ja sitä noudatetaan yleislakina, ellei asiakirjojen käsittelystä ole muualla lainsäädännössä säädetty toisin. (Voutilainen 2012, 58.) Lain 18.§ kuvaa hyvää tiedonhallintatapaa, jonka mukaan organisaatioiden on huolehdittava siitä, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä siitä, miten tietoa voidaan antaa ja käsitellä. Henkilöillä on oltava tieto myös tietojen, asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä ja tietoturvallisuusjärjestelyistä. Lisäksi organisaatioiden on hyvän tiedonhallintatavan toteuttamiseksi valvottava annettujen säännösten, määräysten ja ohjeiden noudattamista. (Laki viranomaisen toiminnan julkisuudesta 1999.)

Viranomaisten toimintaa määrittää myös arkistolaki, jonka mukaan viranomaisten on määrättävä sen tehtävien hoidon tuloksena syntyvien asiakirjojen säilytysajat ja –tavat ja pidettävä niistä arkistonmuodostussuunnitelmaa. Arkistonmuodostussuunnitelma on asiakirjallisen tiedon ohjeisto, jolla taataan julkisuuslain hyvän tiedonhallintatavan toteutuminen. Sen avulla voidaan myös todeta viranomaisen tieto- ja asianhallinnan nykytila. Arkistonmuodostussuunnitelma vaatii tämän johdosta myös jatkuvaa ajan tasalla pitämistä. (Voutilainen 2012, 103 – 105.)

Ammattikorkeakoulujen toimintaa säätelee erikseen vielä ammattikorkeakoululaki, jossa tietojen käsittelyn osalta määrätään muun muassa tietojensaantioikeuksista sekä arkaluonteisten tietojen käsittelystä. Ammattikorkeakoulun tulee pyynnöstä toimittaa opetus- ja kulttuuriministeriölle sen määräämät koulutustiedot sekä annettava opiskelijan terveydentilaa ja toimintakykyä koskevia ja tehtävien hoidon kannalta välttämättömiä tietoja salassapitosäännösten estämättä tietyille viranomaisille. Lisäksi ammattikorkeakoulun tulee määritellä

ne tehtävät, joihin sisältyy arkaluonteisten tietojen käsittelyä ja säilytettävä tiedot erikseen vain niiden henkilöiden saatavilla, joiden tehtäviin tiedon käsittely kuuluu. (Ammattikorkeakoululaki 2014.)

Laki julkisen hallinnon tietohallinnon ohjauksesta eli tietohallintolaki määrää, että julkisen hallinnon viranomaisen on muun muassa suunniteltava oma kokonaisarkkitehtuurinsa ja noudatettava sitä. Lisäksi tietojärjestelmät on saatettava vastaamaan tiedon yhteen toimivuuden kuvauksia. (Laki julkisen hallinnon tietohallinnon ohjauksesta 2011.)

Tietoyhteiskuntakaaressa turvataan sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistetään sähköisen viestinnän tietoturvaa ja palveluiden kehittämistä (Tietoyhteiskuntakaari 2014). Työelämän tietosuojalailla turvataan puolestaan yksityiselämän ja yksityisyyden suoja työelämässä. Laissa on säädetty muun muassa työnantajan oikeuksista käsitellä työntekijän terveydentilaa koskevia tietoja, kameravalvonnasta sekä työntekijän sähköpostin valvonnasta. (Voutilainen, 2012, 57.) Lisäksi asetus tietoturvallisuudesta valtionhallinnossa säätää viranomaisten asiakirjojen käsittelyä koskevista tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja niiden käsittelyssä noudatettavista tietoturvallisuusvaatimuksista (Valtioneuvosto 2010).

Erityisen säännöskeskeistä on henkilötietotietojen käsittely. Henkilötietojen käsittelyn yleislaki on henkilötietolaki, joka sisältää kaikki keskeiset tietosuojaperiaatteet. Merkittävin periaate on se, että henkilötietoja saa käsitellä vain siihen tarkoitukseen, mihin ne on kerätty ja että henkilötietojen käsittely on aina perusteltava. Henkilötietolakia sovelletaan kaikkeen henkilötietojen käsittelyyn, joka tapahtuu tietojärjestelmien avulla sekä henkilörekisteriin kuuluvien henkilötietojen sähköiseen tai manuaaliseen käsittelyyn. (Voutilainen 2012, 56.)

Lainsäädäntö asettaa paljon reunaehtoja organisaatioiden tiedonhallinnalle, mutta ei juurikaan anna käytännön ohjeistuksia tiedonhallinnan laadukkaaseen toteuttamiseen (Hakkarainen-Kiri 2014, 10). Esimerkiksi julkisuuslakia on tulkittu monin eri tavoin, ja sen soveltamiseen on kaivattu ohjeistusta ja koulu-

tuksesta vastaavaa tahoa (Valtiovarainministeriö 2017). Tiedonhallinnan toteuttamista onkin pyritty ohjeistamaan esimerkiksi julkisen hallinnon tietohallinnon neuvottelukunnan suosituksilla ja ohjeilla, jotka perustuvat lainsäädännön velvoitteisiin.

Tietoturvallisuuden osalta myös kansainväliset tietoturvastandardit, kuten ISO27000, ISO27018 ja ISO 27001 ohjaavat toimintaa. Keskeisiä standardisointialueita ovat esimerkiksi tietoturvallisuuden hallintajärjestelmät, salaustekniikat, pääsynvalvonta ja digitaalinen allekirjoitus. Standardien avulla mahdollistetaan yhtenäiset toimintatavat ja tekniikat sähköiseen tietojen vaihtoon ja tietojen käsittelyyn. Niiden avulla voidaan myös varmistaa, ettei tietojärjestelmissä olevia tietoja muuteta ilman valtuuksia ja että tiedot suojataan asiattomalta käytöltä. (Suomen standardisoimisliitto 2017.)

Ammattikorkeakoulut ovat voineet soveltaa tiedonhallinnassaan myös valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän, tietosuojavaltuutetun sekä opetushallituksen ohjeistuksia. Lisäksi henkilötietojen käsittelyn osalta on luotu toimialakohtaisia käytännesääntöjä henkilötietolain soveltamiseen. Korkeakoulujen yhteistyönä on luotu muun muassa opintohallinnon julkisuuteen ja tietosuojaan liittyneet käytännesäännöt.

3.6 Muuttuneen toimintaympäristön vaatimukset tiedonhallinnan lainsäädäntöuudistuksille

Tällä hetkellä voimassa olevien tiedonhallintaa säätelevien lakien on todettu jo jääneen osaltaan digitaalisen maailman jalkoihin ja ne ovat osin vanhentuneet toimintaympäristöään vasten. Lisäksi lukuisten eri lakien tulkintaa on pidetty varsin sekavana. Lainsäädännön uudistamista puoltavat myös hallitusohjelman vaatimukset toiminnan tehostamisesta sekä uuden tekniikan luomat mahdollisuudet. (Valtiovarainministeriö 2017b.) Vaikka toistaiseksi on vielä toimittava voimassaolevan lainsäädännön mukaisesti, on lähivuosien aikana odotettavissa isoja tiedonhallinnon lainsäädännön muutoksia.

Valtiovarainministeriön asettama tiedonhallinnan säätelyn kehittämistyöryhmä (Valtiovarainministeriö 2017b) on ehdottanut lausunnossaan lokakuussa 2017,

että uusi julkisen hallinnon tiedonhallinnan yleislaki yhtenäistäisi tiedonhallintaan liittyvät velvollisuudet ja korvaisi lain julkisen hallinnon tietohallinnon ohjauksesta, arkistolain, osan sähköisestä asioinnista viranomaistoiminnassa annetusta laista sekä osan viranomaisten toiminnan julkisuudesta annetusta laista. Uuden lain tavoitteena on turvata viranomaisten välisten tietojen saatavuus koko tiedon elinkaaren ajalta mahdollisimman vähäisillä tietolupamenettelyillä avoimen tiedon ja rajapintojen avulla. Tiedonhallintaa koskevan yleislain on tarkoitus tulla voimaan vuonna 2019.

25.5.2018 alkaen sovellettava EU:n yleinen tietosuoja-asetus asettaa yhä enemmän vaatimuksia organisaatioille ja antaa oikeuksia tietojen käsittelyn kohteena olevalla henkilölle**.** Asetuksen tarkoituksena on muun muassa vastata teknologian kehitykseen ja globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin, yhdenmukaistaa EU:n jäsenvaltioiden tietosuojaa koskevat säännökset, lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. Yhtenä tietosuoja-asetuksen tärkeimpänä vaatimuksena on osoitusvelvollisuus, jonka mukaan organisaation on pystyttävä näyttämään toteen, että se huolehtii henkilötietojen suojasta kaikessa toiminnassaan. Tarvittaessa valvontaviranomainen voi määrätä henkilötietojen käsittelyyn liittyviä korjaavia toimenpiteitä ja jopa hallinnollisia sakkoja, jos organisaatio ei pysty näyttämään toteen, että asetuksen velvoitteita on noudatettu. (Tietosuojavaltuutetun toimisto 2012.)

EU:n yleinen tietosuoja-asetus jättää jäsenvaltioille jonkin verran kansallista, asetuksen säännöksiä täsmentävää liikkumavaraa. Oikeusministeriö asettama TATTI-työryhmä on ehdottanut mietinnössään, että nykyisen henkilötietolain tilalle säädetään yleislakina uusi henkilötietojen suojaa koskeva tietosuojalaki**,** jolla täsmennetään ja täydennetään EU:n yleistä tietosuoja-asetusta ja joka toimii EU:n tietosuoja-asetuksen rinnalla. Tietosuojalaki on opinnäytetyön kirjoitushetkellä valmisteilla ja sen ehdotetaan tulevaksi voimaan samanaikaisesti EU:n tietosuoja-asetuksen kanssa. (Oikeusministeriö 2017.)

4 TIETOSUOJA JA TIETOTURVA

Tietoturvallisuudella suojataan niin organisaation tietoja kuin luottamuksellista viestintää. Sen avulla julkinen tieto on saatavilla ja salassa pidettävät tiedot vain niihin oikeutettujen käytettävissä. Tietosuoja tarkoittaa puolestaan sekä julkisten että salassa pidettävien henkilötietojen käsittelyä lainsäädännön rajoissa yksilön oikeuksia ja yksityisyyttä kunnioittaen (Voutilainen 2012, 41-51.) Hyvin johdetun tietoturvan ja tietosuojan avulla pystytään varmistamaan ja osoittamaan organisaation toimintakyky ja tietoaineistojen laatu.

Tietoturvaan ja tietosuojaan liittyvien toimenpiteiden avulla voidaan vaikuttaa myös organisaation riskien minimointiin, maineen hallintaan sekä asiakkaiden luottamuksen säilyttämiseen, jotka ovat yhä tärkeämpiä edellytyksiä toiminnassa menestymiselle. Paitsi että tietosuojan ja tietoturvan toteuttaminen on organisaatioille laissa säädetty velvollisuus, on se myös oleellinen osa hyvää palvelua, jolla tietojen liikkuminen prosessista toiseen voidaan toteuttaa sujuvasti ja asianmukaisesti. Henkilötietojen suojan osalta vääriin käsiin joutuneet tiedot ovat puolestaan uhka niin tietojen kohteena olevan henkilön oikeusturvalle kuin tietojen suojauksen laiminlyönnistä vastuullisen organisaation toiminnalle ja maineelle. (Tietosuojavaltuutetun toimisto 2012.)

Tietoturvan ja tietosuojan suhdetta organisaation toimintakyvyn turvaamisen ja maineen hallinnan mahdollistajana kuvaan kuvan 3 keinoin.

Kuva 3. Tietoturva ja tietosuoja organisaation toimintakyvyn ja maineen hallinnan mahdollistajana.

Vaikka tietosuojan velvoitteet, tavoitteet ja periaatteet eroavat osittain toisistaan, limittyvät ne myös toisiinsa. Käytännössä toista ei voi olla ilman toista. Jos tiedot eivät ole turvassa, ei myöskään henkilöiden yksityisyyden suoja toteudu. Tietojen eheys, luotettavuus ja käytettävyys takaavat puolestaan tiedon kohteena olevien rekisteröityjen oikeuksien toteutumisen, ja riskienhallinta kattaa tekniset ja organisatoriset toimenpiteet niin tiedon haitallista käyttöä vastaan kuin henkilötietolainsäädännön noudattamiseen.

4.1 Tietosuojan ja tietoturvan tavoitteet

Tietosuojan ja tietoturvan toimenpiteiden yhteinen tavoite on taata organisaation toimintakyky ja maineenhallinta. Julkishallinnon organisaatioilla on myös tavoitteena osaltaan mahdollistaa koko yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen ratkaisujen toimivuus. Kansalaisten ja asiakkaiden on pystyttävä luottamaan siihen, että heitä koskevaa tietoa käsitellään asianmukaisesti. Kun tietojen käsittely on turvattu ja suojattu, pystytään hyödyntämään myös uutta teknologiaa ja digitalisaatiota täysimääräisesti ja menestymään näin omalla toimialalla.

Tietoturvan avulla suojataan organisaation tarvitsema ja käyttämä tieto, mutta tavoitellaan myös joustavia ja sujuvia asiakasprosesseja. Kun järjestelmissä liikkuva tieto on hallinnassa, ei organisaatiolle aiheudu prosessien tyhjäkäyntiä tai virheellisiä toimintatapoja. Tietosuojan toimenpiteiden tavoitteena on puolestaan henkilöiden perusoikeuksien toteutuminen, mutta yhtenä tavoitteena voi myös pitää henkilökunnan työhyvinvoinnin ja oikeusturvan paranemista. Kun henkilökunta on tietoinen erilaisten henkilötietoryhmien käsittelytavoista, epävarmat toimintatavat vähenevät, mikä osaltaan lisää myös työtehoa ja vähentää kustannuksia. (Andreasson ym. 2017.)

4.2 Tietojen eheys, käytettävyys ja luotettavuus

Tietoturvan ja tietosuojan periaatteet sivuavat monilta osin toisiaan erityisesti tietojen käytettävyyden, eheyden ja luotettavuuden varmistamisen osalta. Tietoturvasta vastaavan tietohallinnon on pystyttävä varmistamaan, että organisaation tarvitsema tieto on häiriöttömästi ja ymmärrettävässä muodossa käy-

tettävissä. Lisäksi tiedon on oltava teknisesti suojattu tahattomalta tai tahalliselta muuttamiselta ja se on oltava luokiteltu niin, että salassa pidettäviin tietoihin on pääsy vain niillä henkilöillä, joilla on käyttöoikeudet kyseisiin tietoihin. (Voutilainen 2012, 118-119.)

Tiedon eheydellä tarkoitetaan tiedon säilyttämistä ajantasaisena, virheettömänä ja muuttumattomana. Tiedon eheys voi kärsiä virheellisten tai luvattomien toimintamallien seurauksena, joten eheyden varmistaminen edellyttää muutosten todennettavuudesta huolehtimista esimerkiksi lokitietojen avulla. Tämän varmistamiseksi tietojärjestelmissä käsiteltäville tiedoille tulee olla määritelty tietojen käsittelysäännöt, jotka kattavat koko niiden elinkaaren (Mt.).

Käytettävyydellä mahdollistetaan, että tiedot ovat niihin oikeutettujen tahojen käytettävissä tai saavutettavissa oikeaan aikaan. Tietosuojan näkökulmasta käytettävyydellä tarkoitetaan henkilötietojen julkisuudesta ja salassapidosta huolehtimista sekä tiedon luovuttamisen ja antamisen prosesseja ja sitä, että työntekijöillä on aina saatavilla tehtäviensä hoidossa tarvitsemansa tieto. (Mt.)

Tiedon suojaaminen mahdollistaa tiedon luottamuksellisuuden. Luottamuksellisuudella tarkoitetaan, että tiedot ovat vain niihin oikeutettujen henkilöiden saatavilla, eikä niitä paljasteta muille. Tietosuojan näkökulmasta se sisältää toimenpiteet, jotka takaavat henkilötietojen suojan, mutta myös sen, että julkinen tieto on saatavilla silloin, kun tiedon käytölle on tarvetta. (Voutilainen 2012,120.)

4.3 Rekisteröityjen oikeudet ja rekisterinpitäjän velvollisuudet

Tietosuojan toimenpiteiden periaatteina on rekisteröityjen eli henkilörekisteriin kuuluvien oikeudet ja rekisterinpitäjän eli henkilötiedon omistajan velvollisuudet. Henkilötietojen suoja on jokaisen ihmisen perusoikeus, jota määritellään lailla ja asetuksilla. Henkilötietoja käsittelevien organisaatioiden velvollisuus on toimillaan varmistettava, että henkilön oikeudet toteutuvat.

Henkilörekisteriin kuuluvalla rekisteröidyllä on oikeus saada tieto henkilötietojensa käsittelyn tarkoituksesta ja luovutuksesta. Hän voi myös halutessaan

tarkastaa, mitä tietoja hänestä on tallennettu eri rekistereihin sekä vaatia rekisterissä olevan virheellisen tiedon korjaamista. (Tietosuojavaltuutetun toimisto 2014.) EU:n tietosuoja-asetuksen soveltamisen myötä toukokuusta 2018 alkaen uusina oikeuksina tulevat voimaan muun muassa henkilön oikeus tulla unohdetuksi. Kun rekisteröity ei enää halua, että hänen tietojaan käsitellään, hänen tietonsa on poistettava järjestelmistä, ellei ole olemassa jotain laillista perustetta niiden säilyttämiseen. Ammattikorkeakouluilla esimerkiksi opiskelijoiden henkilötietojen käsittely perustuu lakisääteiseen opetustehtävään, joten tietoja ei voi poistaa keskeisistä järjestelmistä.

Rekisterinpitäjän velvollisuuksiin kuuluvat rekisteröityjen oikeuksien toteutuminen ja henkilötietojen suojan takaaminen tarvittavin tietoturvakeinoin. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja arvioimaan ja toteuttamaan riskitason mukaisia toimenpiteitä. Rekisterinpitäjän on kerättävä henkilörekisteriin vain niitä henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta. Tietoja ei myöskään saa kerätä tai säilyttää kuin vain sen ajan, kun on välttämätöntä kyseiseen käsittelytarkoitukseen. Lisäksi on varmistettava, että henkilötietoja ei saateta rajoittamattoman henkilömäärän saataville. (Valtiovarainministeriö 2016.) Organisaatioiden on myös jatkossa raportoitava kansalliselle tietosuojaviranomaiselle tietoturvaloukkauksista sekä ilmoitettava käyttäjille vakavista loukkauksista mahdollisimman pian tiedon saatuaan (Tietosuojavaltuutetun toimisto 2016).

4.4 Tiedon julkisuus ja salassapito ammattikorkeakouluissa

Ammattikorkeakoululain 21.2 §:n mukaan ammattikorkeakoulujen toiminnan julkisuuteen sovelletaan julkisuuslakia samalla tavoin kuin viranomaisen toimintaan. Jokaisella on siis oikeus saada tieto ammattikorkeakoulun asiakirjasta, jota ei ole erikseen säädetty salassa pidettäväksi. Ammattikorkeakoulujen velvollisuutena on näin julkisina organisaatioina edistää toimintansa avoimuutta ja pitää yllä hyvää tiedonhallintatapaa. Tämä edellyttää sitä, että julkiset asiakirjat on asianmukaisesti järjestetty, tarvittava tietoaineisto on ajantasaista ja saatavissa ja että toiminta ja tietojen käsittely perustuvat avoimuuteen. (Karppinen & Johansson 2017.)

Ammattikorkeakoulun julkisia asiakirjoja ovat kaikki kirjalliset, kuvalliset ja sähköiset viestit, jotka liittyvät ammattikorkeakoulun tehtäviin ja joita ei ole erikseen määrätty salassa pidettäviksi. Julkisia asiakirjoja ei kuitenkaan ole henkilöstön omaan tai ammattikorkeakoulun sisäiseen käyttöön tarkoitetut asiakirjat. Keskeneräiset asiakirjat eivät ole myöskään pääsääntöisesti julkisia. Pöytäkirjat, päätökset, lausunnot ja sopimukset tulevat julkisiksi, kun ne on allekirjoitettu tai muuten varmistettu. Muilta osin asiakirjat tulevat julkisiksi, kun asia, jota asiakirja koskee, on ammattikorkeakoulussa käsitelty loppuun. (Karppinen & Johansson 2017.)

Viranomaisen salassa pidettävät asiakirjat on määritelty julkisuuslain 24§:ssä. Salassapito tarkoittaa sekä velvollisuutta asiakirjan salassa pitoon, että velvollisuutta olla muutoin ilmaisematta tietoa asiakirjasta tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä. (Karppinen & Johansson 2017.) Luettelen seuraavassa ne lain momentit, jotka sisältävät ammattikorkeakouluissa käsiteltäviä asiakirjoja, ja ovat siten salassa pidettäviä.

6 mom. *kanteluasiakirjat ennen asian ratkaisua,*

7 mom. *henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat*

8. mom. *onnettomuuksiin tai poikkeusoloihin varautumista koskevat asiakirjat*

16. mom. *tilastoviranomaiselle annetut asiakirjat sekä viranomaiselle tutkimusta tai tilastointia varten annetut asiakirjat*

17. mom. *liike- tai ammattisalaisuuksia sisältävä asiakirjat*

18. mom. *asiakirjat, jotka sisältävät työmarkkinaosapuolena tai työriidan osapuolena laatimia tai saamia tietoja*

19. mom. *viranomaisen oikeudenkäynnin osapuolena oikeudenkäyntiin valmistautumista varten laatimat ja hankkimat asiakirjat*

20.mom. *asiakirjat, jotka sisältävät tietoja yksityisestä liike- tai ammattisalaisuudesta.*

21. mom. *opinnäytetyön tai tieteellisen tutkimuksen suunnitelma tai perusaineisto taikka teknologinen tai muu kehittämistyö tai niiden arviointi*

22 mom. *asiakirjat, jotka sisältävät tietoja pääsy- tai muusta kokeesta tai testistä*

23. mom. *henkilön vuosituloja tai kokonaisvarallisuutta taikka tuen tai etuuden perusteena olevia tuloja ja varallisuutta koskevat asiakirjat*

25 mom. *asiakirjat, jotka sisältävät tietoja sosiaalihuollon tai työhallinnon henkilöasiakkaasta sekä tämän saamasta etuudesta, tukitoimesta tai palvelusta taikka tietoja henkilön terveydentilasta tai vammaisuudesta taikka hänen saamastaan terveydenhuollon ja kuntoutuksen palvelusta*

26 mom. *asiakirjat, jotka sisältävät tietoja rikoksesta epäillyn, asianomistajan tai muun rikosasiaan liittyvän henkilön yksityiselämään liittyvistä arkaluonteisista seikoista samoin kuin sellaiset asiakirjat, jotka sisältävät tietoja rikoksen uhrista*

28.mom. *rikosrekisteriin, sakkorekisteriin, oikeushallinnon valtakunnalliseen tietojärjestelmään talletetut tiedot*

29. mom. *asiakirjat, jotka sisältävät tietoja henkilölle suoritetusta psykologisesta testistä tai soveltuvuuskokeesta tai sen tuloksesta tai työntekijän valintaa tai palkkauksen perustetta varten tehdyistä arvioinneista*

30 mom. *oppilashuoltoa ja oppilaan opetuksesta vapauttamista koskevat asiakirjat, oppilaan ja kokelaan koesuoritukset sekä sellaiset oppilaitoksen antamat todistukset ja muut asiakirjat, jotka sisältävät oppilaan henkilökohtaisten ominaisuuksien sanallista arviointia koskevia tietoja*

31 mom. *asiakirjat, jotka sisältävät tiedon henkilön yhteystiedoista, jos henkilö on pyytänyt tiedon salassapitoa ja hänellä on perusteltu syy epäillä itsensä tai perheensä terveyden tai turvallisuuden tulevan uhatuksi.*

32 mom. *asiakirjat, jotka sisältävät tietoja henkilön poliittisesta vakaumuksesta tai tietoja henkilön yksityiselämän piirissä esittämistä mielipiteistä taikka tietoja henkilön elintavoista, osallistumisesta yhdistystoimintaan tai vapaa-ajan harrastuksista, perhe-elämästä tai muista niihin verrattavista henkilökohtaisista oloista.*

(Laki viranomaisen toiminnan julkisuudesta 1999.)

Salassa pidettävä tieto on luokiteltava suojausluokkiin, jotka on määritelty aiheutuvan vahingon perusteella, jonka tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa. Neliportainen suojaustaso on määritelty seuraavasti:

Suojaustaso I: Erittäin salainen.

- Voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.

Suojaustaso II: Salainen.

- Voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.

Suojaustaso III: Luottamuksellinen

- Voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.

Suojaustaso IV: käyttörajoitettu

- Voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.

Luokiteltaessa salassa pidettäviä asiakirjoja edellä mainittuihin suojausluokkiin on otettava huomioon tiedon tarvitsijoiden laajuus. Sellaiset asiakirjat, jotka vaativat laajaa käsittelyä ja joiden paljastumisesta aiheutuva haitta tai luottamuksen menettäminen on vähäistä, luokitellaan suojaustasoon IV. Mitä aremmasta tiedosta on kysymys, sitä korkeampia turvajärjestelyjä edellytetään koko tiedon käsittelyketjulta. (Valtiovarainministeriö 2010.)

Ammattikorkeakouluissa ei käsitellä suojaustason I tietoja, jotka sisältävät lähinnä valtiolliseen turvallisuuteen liittyviä tietoja. Suojaustasoon II kuuluvia tietoja on ammattikorkeakouluissa hyvin vähän, mutta ne ovat erityisen kriittinen tietoryhmä, joita käsitellään erityisesti turvallisuuteen tai rikoksiin liittyvissä asioissa tai näihin liittyvissä erityisissä tutkimus- ja kehityshankkeissa. Arkityössä ammattikorkeakoulujen salassa pidettävä tieto luokitellaan suojaustasojen III ja IV –mukaisiin luottamukselliseen ja käyttörajoitettuun tietoon.

Luottamuksellista tietoa saavat käsitellä vain ne henkilöt, joilla on tietoon työtehtäviensä puolesta tarve, päätösvalta ja jotka tuntevat myös tiedon käsittelyyn liittyvät velvoitteet. Luottamuksellista tietoa ovat muun muassa henkilön terveydentilaa koskeva tieto tai opiskelijoiden rikosrekisteritiedot, joita pyydetään lasten kanssa työskenteleviltä henkilöiltä.

Käyttörajoitetut tiedot ovat vain niihin oikeutettujen käytössä. Tarvittaessa niihin voi olla pääsy asiayhteyden mukaan koko henkilökunnalla, jos he tarvitse-

vat tietoa työssään. Tietoa ei saa kuitenkaan antaa ulkopuolisille ja tiedon käsittelyssä on oltava huolellinen. Esimerkiksi henkilötietolain mukaan henkilötunnuksen sisältäviä asiakirjoja on käsiteltävä suojaustason IV mukaisesti, ellei asiakirjan sisällön perusteella sitä kuulu käsitellä korkeamman suojaustason vaatimusten mukaisesti. (Valtiovarainministeriö 2010.)

Asiakirjojen oikeat luokittelutiedot ovat tärkeitä, koska niiden avulla saadaan tietoa siitä, millaisia vaatimuksia asiakirjojen käsittelyssä tulee noudattaa. Luokittelun merkitys korostuu, kun tietoja luovutetaan joko manuaalisesti tai digitaalisesti organisaation sisällä tai sen ulkopuolelle. (Valtiovarainministeriö 2017b.) Kaikkien salassa pidettävien tietojen säilytykseen ja käsittelyoikeuksiin onkin kiinnitettävä digitaalisessa maailmassa yhä tarkempaa huomiota. Tiedon käsittely on myös ohjeistettava tarkoituksenmukaisin roolein. Lisäksi tiedon antamisen vastuut ja käsittelyprosessit niin julkisesta kuin salassa pidettävästä asiakirjasta on määriteltävä selkeästi.

Valtiovarainministeriön asettama tiedonhallinnan lainsäädännön kehittämistyöryhmä (Valtiovarainministeriö 2017b) toteaa lausunnossaan, että suojausluokittelusäännösten tulkinta ja soveltaminen on koettu vaikeaksi. Asiakirjojen Suojaustason III ja Suojaustason IV erojen tunnistaminen sekä luokittelun perusteena käytettyjen aiheutuvan haitan ja vahingon arvioiminen ovat aiheuttaneet haasteita organisaatioille. Asiakirjojen väärä luokittelu on myös saattanut vaarantaa asiakirjan luottamuksellisuuden tai saatavuuden. Työryhmä ehdottaakin, että salassa pidettävien tietojen luokittelua yksinkertaistetaan uuden tiedonhallintalain myötä. (Mt.)

5 TIEDONHALLINTAOSAAMISEN NYKYTILA LAUREASSA

Laurean tiedonhallintaosaamisen nykytilaa kuvaan Kruger & Kearneyn (2006) mallia ja Karjalaisen (2011) teoriaa mukaillen Laurean henkilöstön osaamisen, toimintatapojen ja asenteiden kautta. Pohjana tietojen kartoitukselle toimii henkilöstölle tehty tietosuoja- ja tietoturvatesti, johon vastasi noin viidesosa henkilöstön jäsenistä. Lisäksi olen haastattelut tutkimustani varten Laurean turvallisuusjohtajaa ja henkilöstöjohtajaa. Olen myös kartoittanut Laurean ole-

massa olevia prosesseja, ohjeita ja koulutuksia sekä havainnoinut nykyistä tiedonhallintaosaamisen tilaa omasta näkökulmastani Laurean henkilökunnan jäsenenä.

5.1 Laurea-ammattikorkeakoulun toiminta ja henkilöstö

Laurea-ammattikorkeakoulu toimii kuudella kampuksella Espoossa, Hyvinkäällä, Lohjalla, Porvoossa ja Vantaalla. Sen koulutusaloina ovat liiketalous, sosiaali- ja terveysala sekä matkailu-, ravitsemis- ja talousala. Opiskelijoita on Laureassa noin 8400, joista AMK-tason opiskelijoita on noin 7700. Henkilöstön määrä on reilu 500, joista opetushenkilöstöä oli vuonna 2016 yhteensä 287 ja tukihenkilöstöä 217. Opetushenkilöstön keski-ikä vuonna 2016 oli 50,9 vuotta ja tukihenkilöstön 42,4 vuotta. (Laurea-ammattikorkeakoulu 2017.).

Laurean toimintaa ohjaa Strategia 2020, jonka mukaan Laurean tahtotila on olla Metropolialueen hyvinvoinnin ja kilpailukyvyn kansainvälinen kehittäjä. Toimintatavat perustuvat puolestaan brändilupaukselle: ”Yhdessä enemmän – Laurea Uudellamaalla”, jossa korostuvat yhdessä tekeminen ja oppiminen. (Laurea-ammattikorkeakoulu 2016.)

5.2 Henkilöstön tietoturva- ja tietosuojatietämyksen osaamistesti

Lähtölaukaus Laurea-ammattikorkeakoulun henkilöstön sitouttamiseen tiedonhallinnan osaamisen kehittämiseen ja EU:n tietosuoja-asetuksen vaatimusten täyttämiseen toteutettiin elokuussa 2017 lukuvuoden aloitusseminaarissa. Päivän yhteydessä pidettiin vapaaehtoisia työpajoja, joista yhden teemana oli tietosuoja ja tietoturva. Muut workshopit liittyivät esimerkiksi TKI-toimintaan, markkinointiin ja aluekehitykseen. Työpajoihin osallistuttiin vapaamuotoisesti noin kahden tunnin aikana, ja niihin osallistui noin 200 laurealaista.

Tietosuoja- ja tietoturvatyöpajaan osallistuneet henkilöt vastasivat 10 eri väitteeseen paperilla, jonka jälkeen vastauksia käytiin läpi henkilökohtaisesti pienissä ryhmissä. Kysymyksistä viisi kuvastivat vastaajan tietoa tietosuojaan tai tietoturvaan liittyvistä aiheista ja viisi kysymystä liittyivät henkilön käyttäytymiseen tai toimintamalleihin. Vastauksia saatiin takaisin 101 kappaletta. Testi it-

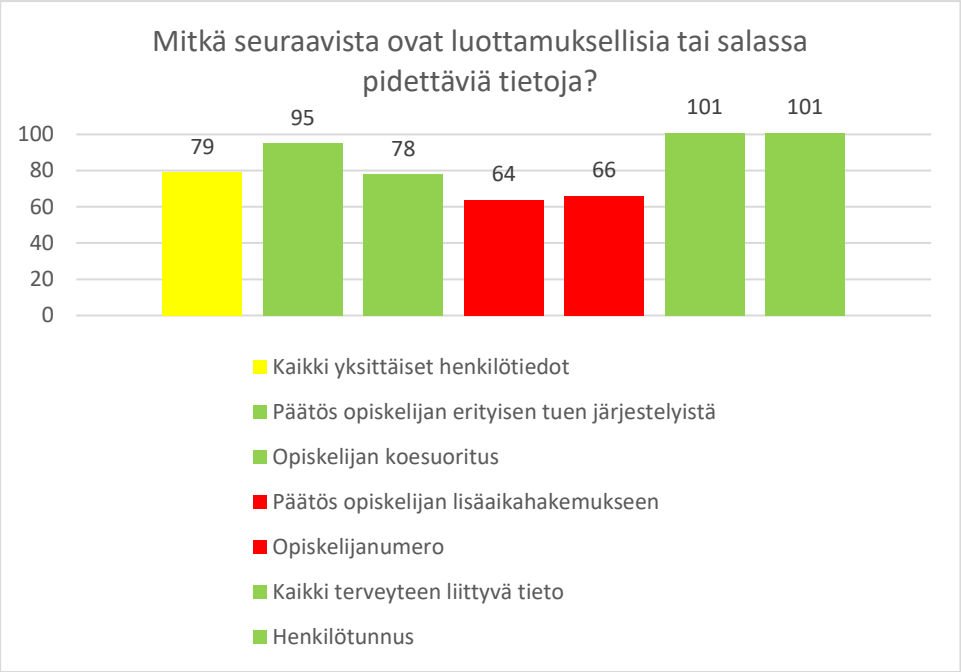
sessään kesti keskimäärin kymmenen minuuttia, mutta erityisesti sen jälkeinen keskustelu koettiin hyödyllisenä ja ajatuksia herättävänä. Osallistujien asenne tietosuojaa ja tietoturvaa kohtaan oli yllättävänkin positiivinen.

Workshopin tavoitteena oli herättää keskustelua, mutta myös saada käsitys henkilöstön osaamistasosta ja toimintamalleista. Niiden tulokset toimivat myös pohjana koulutustarpeiden kartoitukselle ja erilaisille ohjeistuksille. Kysymyslomakkeissa ei kuitenkaan kysytty vastanneiden taustatietoja, joten esimerkiksi opetus- ja tukihenkilöstön osaamistasojen erosta ei voi kyselyn perusteella tehdä erillisiä päätelmiä. Yleisellä tasolla tulokset antavat kuitenkin viitteitä koko henkilöstön tiedonhallinnan osaamistarpeista ja toiveista.

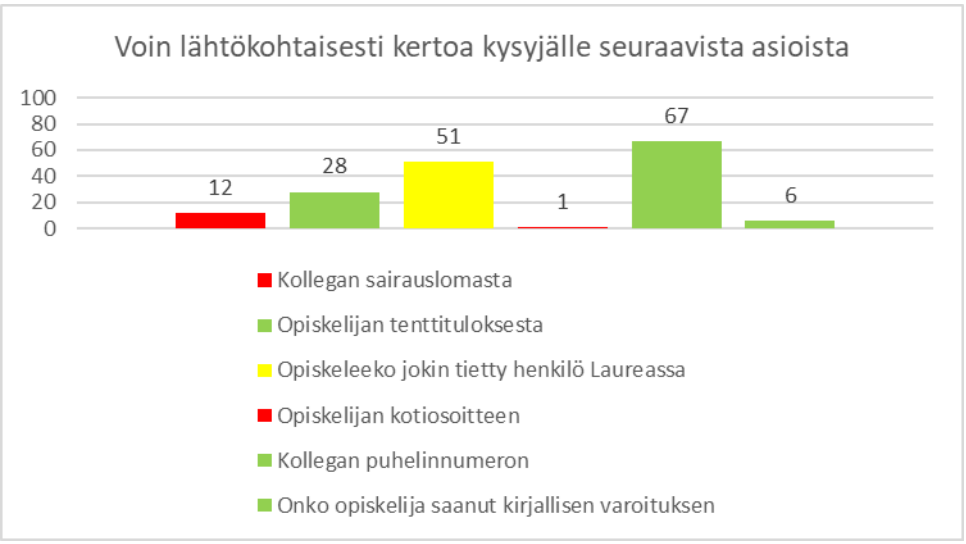
Tiedon osa-alueista selkeimpänä osaamisvajeena nousi esiin tiedon julkisuuteen ja salassapitoon liittyvä tematiikka ja toisaalta tietoturvallinen viestintä. Kaikki vastanneet tunnistivat, että henkilöiden terveystiedot ja henkilötunnus ovat luottamuksellista tietoa, mutta tiedon antamiseen liittyviä käytänteitä ei tunnettu kovinkaan hyvin. Vastanneista 12 prosentilla tuli esimerkiksi yllätyksenä se, että tieto henkilön sairauslomasta on luottamuksellinen tieto. Työnantajalla ei siis ole lähtökohtaisesti oikeutta kertoa sairauspoissaolosta muille työntekijöille.

Lisäksi 49 % vastanneista oletti, että opiskelijan läsnäolotietoa ei voi kertoa kysyjälle. Vastaus oli oikein ja väärin, sillä kirjoilla olevat opiskelijat ovat julkista tietoa, mutta opiskelijan ilmoittama turvakielto on este tiedon antamiselle, joten tietoa ei voi antaa ennen kuin turvakiellon mahdollinen olemassaolo on tarkastettu opiskelijatietojärjestelmästä. Lähes kolmasosa (28 %) vastanneista oletti myös, että opiskelijan tenttinumero on salassa pidettävä tieto. Julkisuuslain mukaan kuitenkin ainoastaan tenttisuoritus ja sanallinen arviointi ovat salassa pidettäviä, kun taas numeerinen arvosana voidaan antaa pyydettäessä.

Henkilöiden vastaukset olen koonnut pylväsdiagrammeihin, joita kuvastavat liikennevalojen värit. Vihreä väri kuvaa oikeaa vastausta tai toimintatapaa, punainen virheellistä ja keltainen tapaa, jossa ei ole selkeää oikeaa tai väärää vastausta, vaan on syytä pysähtyä miettimään, mikä tilanteessa on oikein. Vastaukset tiedon salassapitoon ja julkisuuteen liittyen on koottu kuviin 4 ja 5.

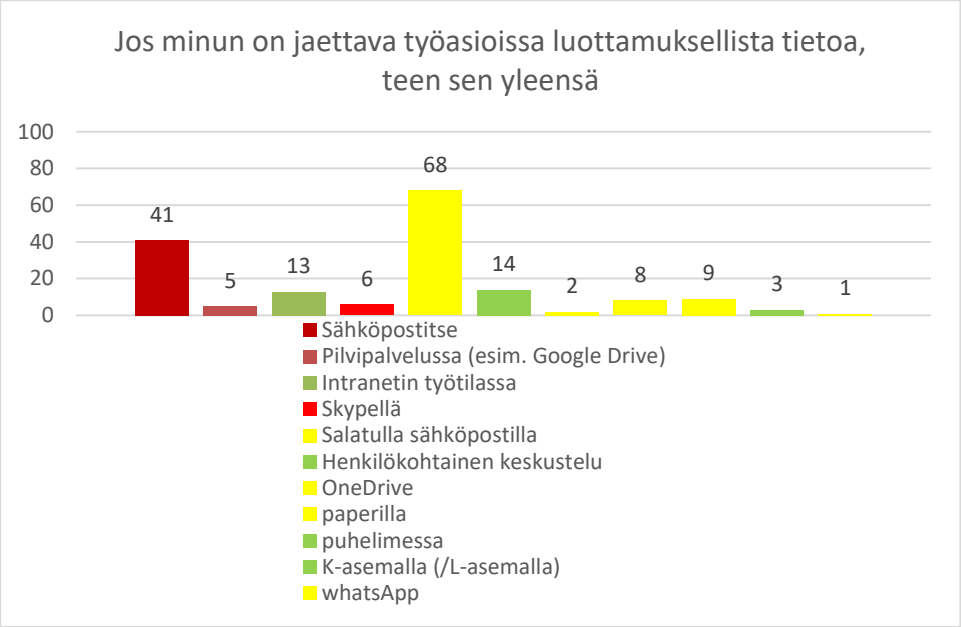


Kuva 4. Henkilöstön osaamistesti: Tietojen luottamuksellisuus.



Kuva 5. Henkilöstön osaamistesti: Tietojen julkisuus.

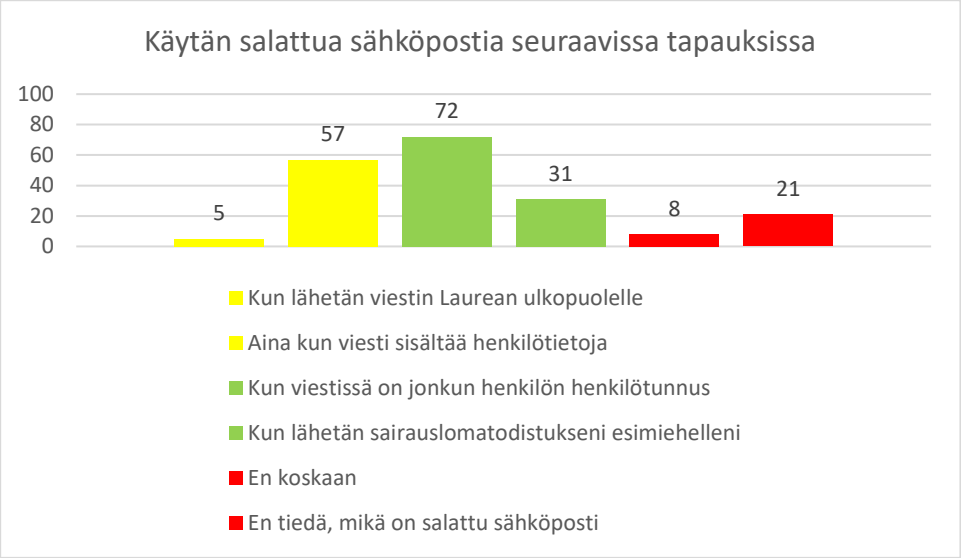
Luottamuksellisen viestintään liittyen suurin osa henkilöstöstä jakoi tietoa sähköpostitse tai salatulla sähköpostilla (kuva 6). Vastausten perusteella sähköpostin tietoturvariskejä ei tunnisteta ja vaikka 68 % käyttää salaista sähköpostia, olisi kuitenkin hyvä pysähtyä miettimään, onko sähköposti ylipäätään oikea tapa jakaa luottamuksellista tietoa. Valmiissa vastausvaihtoehdoissa ei ollut valmiina kasvokkain tapahtuvaa tiedon jakamista, joten henkilöiden itse lisäämää 14 % osuutta voi pitää tässä tapauksessa hyvänä määränä. Vastausten moninaisuus kuitenkin osoittaa, että luottamuksellisen tiedon jakamisen riskeihin ei kiinnitetä riittävästi huomiota.



Kuva 6: Henkilöstön osaamistesti: Luottamuksellisen tiedon jakaminen.

Tietoturvallisen viestinnän osalta käytiin testin jälkeen erityisen paljon keskustelua siitä, miten ja milloin pitäisi käyttää salattua sähköpostia. Salatun sähköpostin käyttämiseen liittyvässä kysymyksessä (kuva 7) 70 % rastitti vastausvaihtoehtona olleen viestin sisältämän henkilötunnuksen, jonka Laureassa käytössä oleva salattu sähköpostijärjestelmä tunnistaa automaattisesti. Lähes 55% vastanneista kertoi käyttävänsä salattua sähköpostia aina, kun viesti sisältää henkilötietoja. Tilastojen perusteella luku ei ole kuitenkaan näin suuri, ja voikin päätellä, että henkilötiedot on tässä tapauksessa tulkittu arkaluonteisiksi henkilötiedoiksi tai muuten luottamuksellisiksi tiedoiksi.

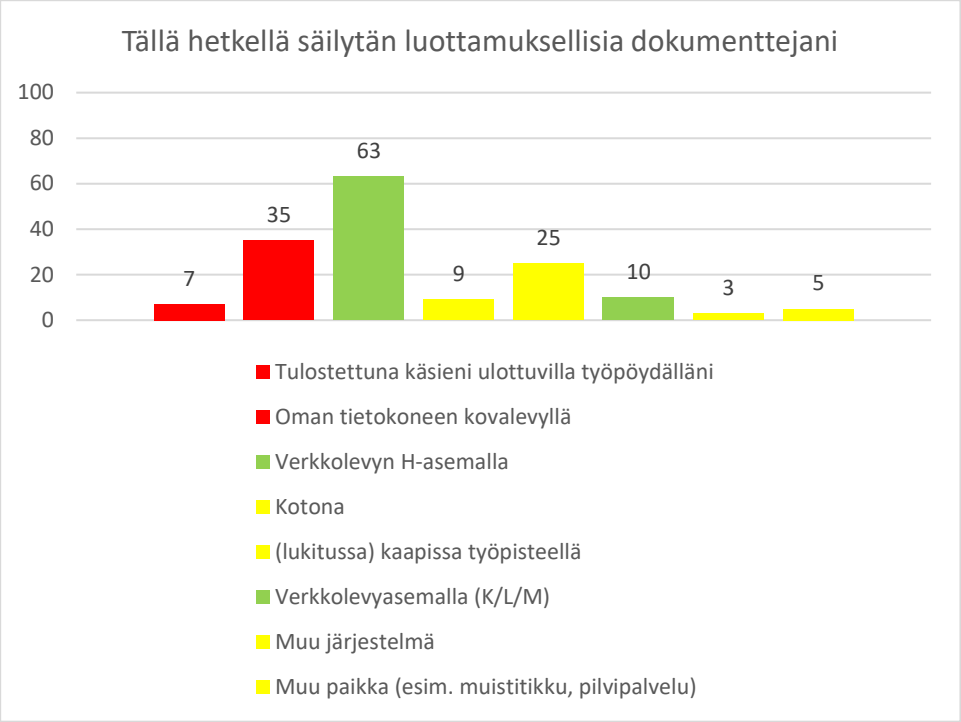
Toisaalta 21 % vastanneista ei tiennyt, mikä on salattu sähköposti ja 8 % vastanneista tiesi salatun sähköpostin olemassaolosta, muttei käyttävänsä sitä koskaan. Vastausten perusteella voi päätellä, että salatun sähköpostin käyttötarkoituksesta ja olemassaolosta ei ole tiedotettu henkilöstöä riittävällä tavalla.



Kuva 7. Henkilöstön osaamistesti: Salattu sähköposti

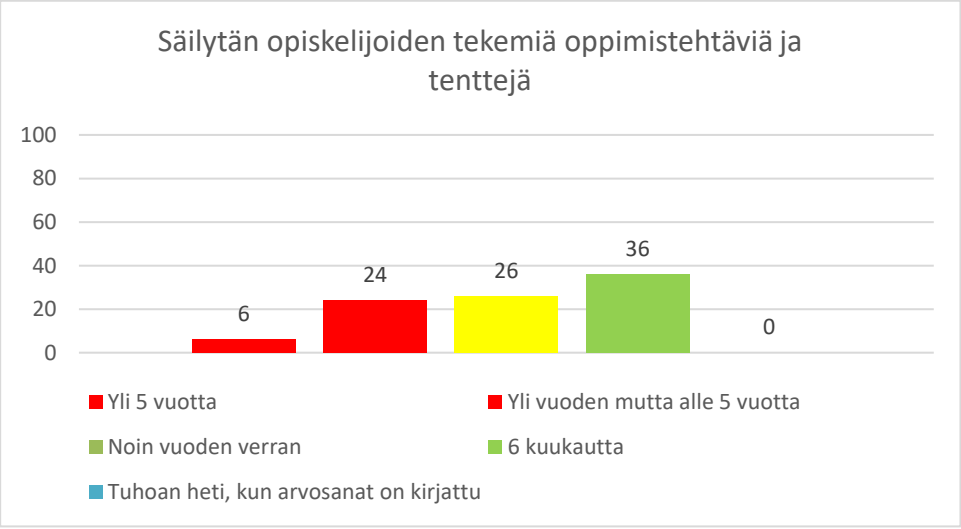
Käyttäytymistä mittaavista väitteistä nousi esille se, että henkilöstö kertoi säilyttävänsä luottamuksellista tietoa yhteensä yhdessätoista eri paikassa, kun mukaan lasketaan vastaajien itse lisäämät vaihtoehdot, muun muassa eri yhteiskäyttöiset verkkolevyasemat (kuva 8). Henkilöt rastittivat lomakkeelle kaikki ne paikat, joissa säilyttävät luottamuksellisia tietoja. Keskimäärin säilytyspaikkoja oli kaksi, ja yleisin paikka oli henkilökohtainen verkkolevyasema. Huolestuttavana voi pitää tulosta siitä, että 16 % vastaajista kertoi tallentavansa luottamuksellista tietoa ainoastaan tietokoneensa kovalevylle.

Vastaukset osoittavat, että yhtenäistä toimintamallia luottamuksellisen tiedon säilyttämiselle ja tallentamiselle ei ole tällä hetkellä olemassa. Laureassa ei ole käytössä asianhallinta- eikä dokumenttienhallintajärjestelmää, joten sähköisten asiakirjojen yhtenäistä säilyttämistapaa ei tueta myöskään järjestelmätasolla.



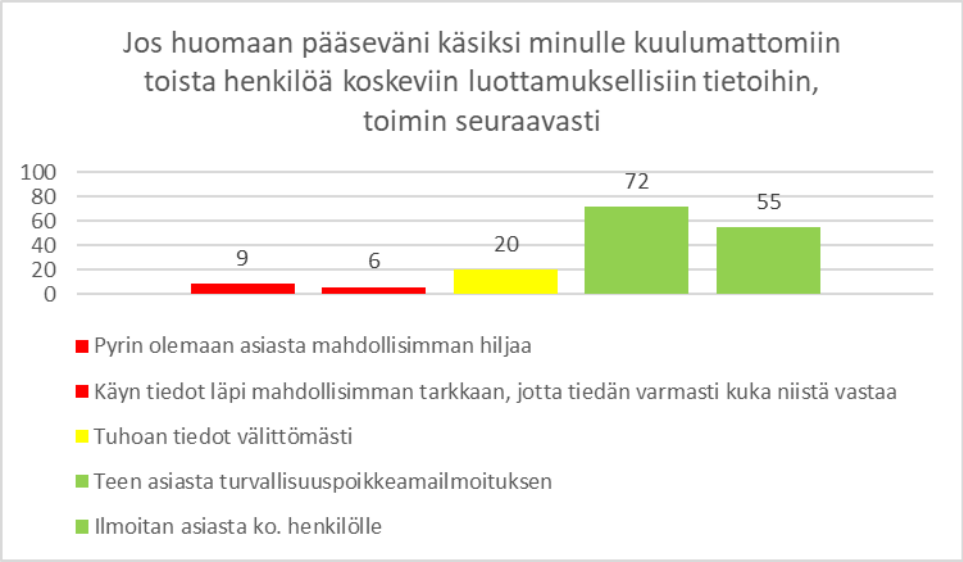
Kuva 8. Henkilöstön osaamistesti: Dokumenttien säilytys

Dokumenttien säilytykseen liittyi myös esimerkkikysymys siitä, kuinka kauan lehtorit säilyttävät opiskelijoiden opintosuorituksia (kuva 9). Myös tähän kysymykseen vastattiin varsin laajalla skaalalla. Osa vastaajista tosin sanoi suoraan, että he arvasivat vastauksen, koska asia ei heitä koske ja osa tukipalveluihin kuuluvista henkilöistä jätti vastaamatta kysymykseen kokonaan. Vastausten hajonta kuvastaa kuitenkin hyvin sitä, että Laurean arkistonmuodostussuunnitelma ei ole tällä hetkellä voimassa, eikä ohjaa tiedon elinkaaren hallintaan.



Kuva 9. Henkilöstön osaamistesti: Tenttien säilytys.

Myös osa käyttäytymiseen liittyneistä kysymyksistä oli sellaisia, joihin ei ollut selkeää oikeaa tai väärää vastausta. Kysymykseen siitä, miten henkilö toimii huomatessaan pääsevänsä käsiksi itselleen kuulumattomaan tietoon (kuva 10), 20 % vastanneista kertoi tuhoavansa tiedot heti. Tämä voi olla hyvä toimintamalli, jos kyse on esimerkiksi kopiohuoneeseen jääneistä luottamuksellisista papereista, mutta esimerkiksi sähköisissä järjestelmissä on parempi varmistaa, ettei tuhoa jotain tärkeää tietoa. Vain 53 % kertoi ilmoittavansa asiasta kyseistä tietoa koskevalle henkilölle. Toisaalta 72 % vastanneista kertoi tässä yhteydessä tekevänsä Laureassa käytössä olevan sähköisen turvallisuuspoikkeamailmoituksen, mitä voi pitää hyvänä osuutena.



Kuva 10. Henkilöstön osaamistesti: Itselle kuulumaton tieto.

Testin jälkeen henkilöt arvioivat myös omaa osaamistaan värikoodein, joista vihreä tarkoitti lähes täydellistä ymmärrystä tiedon hallinnasta, keltainen hieman vajavaista ja punainen selkeästi riittämätöntä tietoa tiedon hallinnan käytännöistä. Noin 80 prosenttia osallistuneista valitsi keltaisen värikoodin. Täydellisesti tiedonhallintaa osasi omasta mielestään noin 10 % osallistuneista ja selkeää osaamisvajetta koki myös noin 10% osallistuneista. Testi ja sen jälkeinen vastausten läpikäynti osoitti konkreettisesti myös vastaajille sen, miten tärkeää on osata tiedonhallintaan liittyviä kysymyksiä.

Työpajassa testi tehtiin paperilla, jotta vastauksia pystyttiin käsittelemään yhdessä pienissä ryhmissä ajatuksia jakaen. Paperille sai myös jättää terveisiä tai muita ajatuksia. Avointen vastausten perusteella testi koettiin tärkeänä ja

koulutusta toivottiin erityisesti esimiehille mutta myös kohdennettuja tietoiskuja eri kohderyhmille. Koko osaamistesti kysymyksineen on liitteessä 1.

5.3 Tietosuoja ja tietoturva osana kokonaisturvallisuutta

EU:n tietosuoja-asetuksen myötä korkeakoulut ovat aloittaneet yhteistyön asetuksen vaatimusten toimeenpanoon. Nykytilan kartoitusta seurataan kypsyystasomallilla, johon sisältyy muun muassa henkilörekistereiden ja henkilötietoja sisältävien prosessien kartoitus. Työn toteuttamista varten Laureaan nimitettiin keväällä 2017 tietosuojavastaava, joka toimii yhteistyössä tietoturvavastaavan kanssa. Tietosuojavastaavan tehtävänä on seurata lainsäädäntöä, ohjeistaa ja kouluttaa henkilöstöä sekä seurata toimintaa niin, että se täyttää lainsäädännön vaatimukset. Lisäksi syksyllä 2017 toimintansa aloitti tietoturva- ja tietosuojaohjausryhmä. Ohjausryhmän tehtäviksi on määritelty tietosuojan ja tietoturvan hallinnollinen kehittäminen, riskienhallinta ja viestintä. Ohjausryhmän puheenjohtajana toimii tietohallintojohtaja ja siihen kuuluu tietosuoja- ja tietoturvavastaavan lisäksi turvallisuusjohtaja, verkko-opetuksen asiantuntija, opetuksen edustaja, sekä markkinointi- ja yhteiskuntasuhteiden johtaja.

Laurean turvallisuusjohtaja näkee kokonaisturvallisuuden näkökulmasta tiedonhallintaan liittyviksi haasteiksi erityisesti arkaluonteisen tiedon suojaamisen ja käsittelyn prosessit. Opiskelijoiden terveystietoja saattaa liikkua prosesseissa niin, että niihin pääsee käsiksi henkilöt, joilla ei ole siihen oikeutta. Henkilöt eivät kuitenkaan ymmärrä tilanteen vakavuutta. Lisäksi on havaittu, että henkilöstö puhuu varomattomasti arkaluonteisista asioista. Arkaluonteista tietoa saatetaan säilyttää myös työpöydällä tai lukitsemattomassa kaapissa. Arkaluonteisten tietojen käsittelystä ja vastuista on tehty rehtorin päätös vuodelta 2013. Dokumentti ei kuitenkaan ole tällä hetkellä yleisesti saatavilla, vaan turvallisuusjohtajan omissa tiedostoissa.

5.4 Perehdyttäminen

Laureassa HR:n rooli on antaa puitteet uuden henkilön perehdytykselle, mutta varsinainen vastuu on esimiehillä, jotka vastaavat osaltaan Laurean perehdytysohjelman käynnistämisestä. Sen jälkeen perehdytys toteutuu nimetyn lä-

hiohjaajan tukemana ja siten, että uusi työntekijä käy itsenäisesti läpi perehdytysohjelmaa. Lisäksi Laurean HR-palvelut järjestävät tulokastilaisuuden kerran vuodessa. Tilaisuus on tarkoitettu kaikille uusille laurealaisille tai pitkiltä vapailta palaaville. Tulokastilaisuudessa käydään läpi Laureaa organisaationa, työsuhdeasioita, turvallisuutta Laureassa sekä muita ajankohtaisia asioita.

Virallisessa perehdytyksessä hyvän tiedonhallinnan mukaista tietojenkäsittelyä on sivuttu lyhyesti osana tietoturvallisuutta. Sitä ei kuitenkaan ole otettu johdonmukaiseksi osaksi perehdytysohjelmaa. Koska lähiohjaajia ei ole erikseen koulutettu ohjaamaan kollegaansa, riskinä saattaa myös olla, että kertoessaan käytännön asioista lähiohjaaja voi jakaa vääriä tiedonhallinnan toimintamalleja ja –tapoja. Henkilöstöjohtaja näkee tiedonhallinnan haasteena myös uusien esimiesten perehdyttämisen. Usein oletetaan, että johtotehtäviin valitut osaavat jo kaiken vanhalta pohjalta, joten esimiesten perehdyttäminen jää puutteelliseksi myös tiedonhallinnan osalta.

5.5 Osaamisen johtaminen

Vuonna 2016 Laureassa määritettiin osana strategista Osaaminen 2020-hanketta henkilöstön 12 strategialähtöisiä osaamisaluetta, joita edellytetään toiminnassa onnistumiseksi ja joiden avulla saavutetaan strategiassa asetetut tavoitteet. Yksi tavoitteista on digiosaaminen, joka kattaa teknologian ja laaja-alaisen viestintätekniikan hyödyntämisen. Osaamisen avulla taataan helposti saatavilla olevat korkeakoulupalvelut sekä tukea opiskelijoiden oppimiseen. Tavoitetta edistää Digitalisaatio2020-työryhmä, joka valmistelee Laurean digitalisaation visiota ja tiekarttaa. Digitalisaatiotyössä on kuitenkin huomioitava, että pelkkä tekninen osaaminen ja innostus uusiin toimintatapoihin ei takaa toiminnassa menestymistä, vaan henkilöstön on tunnettava myös tiedonhallinnan käytänteet, jotta he voivat hyödyntää digitaalista tietoa turvallisesti lain ja asetusten sallimissa rajoissa.

Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän VAHTI-ohjeiden mukaan organisaatioiden johdon tulee huolehtia henkilöstön tietoturvaosaamisen sekä tietoturvakulttuurin ja -tietoisuuden jatkuvasta kehittämisestä. Johdon vastuulla on varmistaa, että jokaisella työntekijällä on tehtäviensä edellyttämä tietoturvallisuuden osaaminen. Osana digiosaamisen taitoja laurealaisille

tarjottiin syksyllä 2016 mahdollisuus testata tietoteknistä osaamistaan tasotestillä. Nettitestin teki 60 laurealaista. Tietoturvaan liittyvien vastausten keskiarvo oli neliportaisella asteikolla 2,7. Vaikka vastanneiden määrä jäi kohtalaisen pieneksi, testi osoitti, että tietoturvallisissa toimintatavoissa on vielä opittavaa.

Alaistensa tietoturvallisuuden edistämiseksi esimiehille tarjottiin keväällä 2017 tietoturvallisuuteen liittynyt koulutusiltapäivä. Koulutukseen osallistui noin 10 Laurean 45:stä esimiehestä. Tämä osaltaan kertoo esimiesten kiireisestä aikataulusta mutta myös esimiesten asenteesta työssä priorisoitaviin asioihin, joissa tietoturvallisten toimintatapojen opettelu ei ole ensimmäisenä listalla. Jotta esimiehet voivat toimia esimerkkeinä alaisilleen, olisi heidän kuitenkin osoitettava se myös teoin.

Osaamisen tueksi koko henkilöstölle Laureassa on käytössä myös pedaohjelma. Siihen kuuluu yksittäisiä koulutuspäiviä, työpajoja ja kehittämistä. Tavoitteena on kehittää Laurean strategian mukaista pedagogista osaamista sekä lisätä yhteistä ymmärrystä pedagogisista muutoksista ja vaatimuksista. Pedagogiseen koulutukseen on vuodelle 2017 varattu kaikille opettajille vähintään 25 tuntia. Myös tukihenkilöstö voi osallistua pedakoulutuksiin. Vuoden 2017 pedaohjelmaan on kuulunut uusien järjestelmien käyttökoulutusta, uudistettujen opetussuunnitelmien tunnettuuden edistämistä, TKI-hankkeiden integrointia opetukseen sekä digitalisaation haasteisiin vastaamista. Varsinaisia tietojen käsittelyyn, tietoturvallisuuteen tai tietosuojaan liittyviä koulutuksia ei pedaohjelman puitteissa ole järjestetty.

Tukihenkilöstön osalta koulutusta järjestetään lähinnä tiimikokousten yhteydessä. Esimerkiksi korkeakoulujen yhteistyönä luodut opintohallinnon julkisuus ja tietosuoja –käytännesääntöjä on käyty opintotoimistojen henkilöstön kanssa lokakuussa 2017.

5.6 Hyvä tiedonhallinta ja viestintä

Tietojen käsittelyyn liittyviä ohjeita on koottu Laurean intranetiin ja osittain tietohallinnon Service-portaaliin. Kävin selvitystäni varten intran ja Service-portaalin sisällöt läpi ja poimin sieltä kaikki tietojenkäsittelyyn liittyvät ohjeistukset, ja sisällöt.

Tietojenkäsittelyyn liittyvät ohjeet on pääosin koottu Intran Turvallisuus-otsikon alla olevan tietoturvaosioon. Tietoturvasivusto jakautuu alaotsikoihin Tietoturvapolitiikka, Tietoturvaohje, Tietoaineistojen käsittely tietojärjestelmissä, Tietoliikenne, Tietosuoja ja Tietotekniikkapalveluiden käyttö. Sivujen sisältö on kohtalaisen ajantasaista, mutta asioita voi olla vaikea löytää monen klikkauksen takaa. Ohjaavia dokumentteja sivuille on koottu seuraavista aiheista:

- Tietoturvaopas henkilökunnalle (päivitetty 2015)
- Tietoturvapolitiikka (päivitetty 2017)
- Rikostaustaotteen tarkistamisohje (päivitetty 2017)
- Tietoaineistojen käsittely tietojärjestelmissä (päivitetty 2014).

Tietoaineistojen käsittelystä tietojärjestelmissä on tehty kuvaus, jolla on pyritty ohjeistamaan tietojen tallentamiseen eri sovelluksiin kuvan 11 mukaisesti. Ohjeistuksessa ei ole kuitenkaan avattu, mitä julkiset, käyttörajoitetut ja luottamukselliset tiedot tarkoittavat konkreettisella tasolla.

Kuva 11. Tietoaineistojen ja sovellusten käyttötavat Laureassa (Laurea-ammattikorkeakoulu 2017).

Intran lisäksi ohjeita on Laurean Service-portaalissa, josta voi lähettää tukipyyntöjä IT:lle, mutta johon on myös koottu erilaisia tietohallinnon käytännön ohjeita. Ohjesivusto on otettu käyttöön Laureassa vuonna 2015 ja tällä hetkellä erilaisia ohjeita on noin 300. Haetuimmat ohjeet käsittelevät Office-pakettien asennusta, Microsofin pilvipalveluita, erilaisten järjestelmien käyttöohjeita sekä mobiilikäyttöä.

Tietoturvaan, tietosuojaan ja yleiseen tietojenkäsittelyyn liittyvinä ohjeina voi pitää seuraavia:

- Onko eLomake tietoturvallinen järjestelmä?
- Matkapuhelinten tietojen suojaaminen
- Tiedostojen varmuuskopiointi H-asemalle
- Uuden henkilön IT-opas
- Google-tunnusten luonti ja kolmannen osapuolen käyttöehtojen hyväksyntä
- Salattu Sähköposti

Service-Portalin ohjeistuksissa on tekninen painotus, mutta ohjeisiin olisi hyvä lisätä myös hyvän tiedonhallinnan käytännön ohjeita ainakin julkisen ja salassa pidettävän tiedon käsittelyyn eri järjestelmissä sekä mobiiliin tiedonhallintaan.

Koska Laurean arkistonmuodostussuunnitelma on keskeneräinen, ei kaikkia asiakirjoja ole luokiteltu julkisiin ja salassa pidettäviin eikä salassa pidettäviä asiakirjoja luottamuksellisiin ja käyttörajoitettuihin suojaustasoihin. Kaikille asiakirjoille ei ole myöskään määritelty säilytysaikoja ja -paikkoja. Arkistonmuodostussuunnitelma ei puutteellisenakaan ole tällä hetkellä henkilöstölle nähtävänä. Tämä kaikki vaikuttaa siihen, että asiakirjoja käsitellään oman työn kannalta parhaaksi katsotulla tavalla, mikä ei välttämättä tue tiedon elinkaaren hallintaa eikä yleisesti Laurean tiedonhallintaa. Arkistonmuodostussuunnitelman päivitystyö on kuitenkin käynnissä. Sen tarkoitus on tukea myöhemmin myös tiedonohjaussuunnitelmatyötä.

Laurean prosessit on kuvattu laadunhallinnan ja kokonaisarkkitehtuurin QPR-järjestelmään. Parhaimmillaan prosessikuvaukset toimivat perehdytyksen välineenä myös tiedonhallinnalle. Tällä hetkellä järjestelmässä on kuitenkin päivittämätöntä tietoa, eikä prosesseissa kulkevaa tietoa ole kytketty prosesseihin. QPR:n hyödyntämisen mahdollisuuksia selvitellään kuitenkin parhaillaan järjestelmäarkkitehdin ja tietopalvelupäällikön kanssa.

Tässä opinnäytetyössäni kartoitin kaikki yleisesti saatavilla olevat ohjeet. Tarpeen olisi kuitenkin myös kartoittaa myös muut mahdolliset kirjoitetut tai kirjoittamattomat ala- / yksikkökohtaiset ohjeistukset esimerkiksi haastattelemalla esimiehiä.

6 HENKILÖSTÖN TIEDONHALLINTAOSAAMISEN TAVOITETILA

Opinnäytetyön tavoitteena on luoda suunnitelma, jonka avulla tietosuoja ja tietoturva tuodaan luonnolliseksi osaksi ammattikorkeakoulun henkilöstön arkipäivää. Hyvän tiedonhallinnan avulla toimintojen läpinäkyvyys lisääntyy, mikä puolestaan lisää työviihtyvyyttä, prosessien toimivuutta ja tehokkuutta. Toimintamallin avulla jokainen uusi henkilö perehdytetään tietosuoja-asioihin ja vanhoilla työntekijöillä on mahdollisuus saada tarvitsemaansa koulutusta ja tietoa.

Yleisen tavoitetilan määrittää lainsäädäntö, EU:n yleisen tietosuoja-asetuksen vaatimukset sekä yleiset velvoitteet ammattikorkeakoulun toiminnassa sekä Laurean strategiset tavoitteet. Osaamisen johtamisen kannalta on tärkeää määritellä, mitkä asiat ovat niitä, mitä koko henkilöstön pitää tietää, mitkä asiat ovat sellaisia, jotka henkilö voi kysyä muilta ja mitkä asiat eivät kuulu omaan työhön. Vähimmäisvaatimuksina on, että tiedon salassapitoasiat ja luottamuksellisen tiedon käsittelyyn liittyvät toimintatavat ovat kaikkien tiedossa ja että henkilöt tietävät oman roolinsa tiedon suojaamisessa ja turvaamisessa.

Tietoturvallisuuden osalta tavoitetilaa voi peilata myös kansallisen turvallisuusauditointikriteeristön (KATAKRI) kohdan A 806.00 –kohdan kriteereihin, joilla varmistetaan organisaation riittävä ohjeistus, koulutus ja tiedotus.

Perustasoon yltääkseen Laurean on varmistettava seuraavat kohdat

1. *Henkilöstö on saanut perehdytyksen yhteydessä ohjeet, kuinka toimia organisaation turvaperiaatteiden mukaisesti. Ohjeistuksen/koulutuksen tulee sisältää tärkeimmät toimintatilanteet (peruskäyttö, etäkäyttö, matkatyö, ylläpito, jne.) ja -tavat.*
2. *Henkilöille, jotka on otettu palvelukseen sellaiseen asemaan, jossa he voisivat päästä suojattaviin tietoihin, annetaan heti aluksi ja säännöllisin väliajoin tarkat ohjeet turvatoimien tarpeellisuudesta ja niiden täytäntöönpanomenettelyistä.*
3. *Suojattavia tietoja käsitteleviin järjestelmiin on laadittu turvallisen käytön ohjeistus.*
4. *Tiedon merkitsemistä (luokittelua), käsittelyä (sis. salaus) ja tallennusta koskeva ohjeistus on laadittu ja otettu käyttöön.*

5. *Henkilöstö on ohjeistettu ja velvoitettu ilmoittamaan havaitsemistaan tietoturvapoikkeamista ja -uhista.*
6. *Tulevista työasemien tietoturva-aukkojen päivityksistä tiedotetaan vähintään sillä tarkkuudella, että käyttäjät ovat tietoisia siitä, mitä toimia heiltä vaaditaan.*
7. *Käyttäjille tiedotetaan kaikkein merkittävimmistä ajankohtaisista uhista, jotka kohdistuvat organisaation käyttäjiin (esim. kohdistetuista hyökkäyksistä).*
8. *Järjestelmien ylläpitohenkilöstö on suorittanut ko. järjestelmiä koskevan turvallisuuskoulutuksen tai ylläpitohenkilöstölle on muuten hankittu riittävä osaaminen ko. järjestelmien turvalliseen ylläpitoon.*

(Puolustusministeriö 2011.)

On kuitenkin huomioitava, että tietoturvallisuuden perustason saavuttaminen ei kuitenkaan takaa sitä, että voisi sanoa asioiden olevan hyvin. Kehittämistyöni tavoite on edistää Laurea-ammattikorkeakoulun tiedonhallintaa henkilöstön osaamista kehittämällä, joten on myös käytävä läpi prosesseja, toimintamalleja ja seurattava ohjeiden noudattamista ja osaamisen karttumista. Olennaista on priorisoida toimenpiteet ja lähteä liikkeelle määrätietoisin askelin kohti henkilöstön strategista tavoitetilaa. Näin lopulta saavutetaan toivottuja hyötyjä.

Hyvän tiedonhallintatavan varmistamiseksi olen määritellyt Laurean näkökulmasta sen perusosaamisen, jonka jokaisen laurealaisen on tiedettävä jokapäiväisessä arkityössään. Perusosaamisen lisäksi on määriteltävä osaamisvaatimukset luottamuksellista ja kriittistä tietoa käsitteleville henkilöryhmille sekä vastuuhenkilöille. Tähän liittyvät esimerkiksi tutkimus- ja kehitystyöhön liittyvä sensitiivisen tiedon käsittely, henkilöstöhallinnon erityispiirteet, esimiestyö ja tiedon osa-alueiden omistajat. Koska nämä tiedot eivät koske kaikkia laurealaisia, olen rajannut nämä osaamisalueet tästä kehittämistyöstä pois.

Tavoitetilassa jokainen laurealainen tietää:

- omaan työhönsä liittyvien dokumenttien turvalliset ja suojatut käsittelypaikat kuten verkkolevyasemat ja Laurean ylläpitämät pilvipalvelut ja työtilat
- kenen vastuulla omaan työhön liittyvien asiakirjojen arkistointi tai hävittäminen on
- miten omaan työhön liittyvää julkista/sisäistä tietoa on käsiteltävä, jotta tiedot ovat tarvittaessa myös muiden saatavilla

- omaan työhönsä liittyvän julkisen tiedon antamisen ja luovuttamisen käytännön tavat sekä sen, kuka tiedon antamisesta tarvittaessa päättää
- salassa pidettävien tietojen huolelliset käsittelytavat niin sähköisesti, paperilla kuin suullisesti
- salatun sähköpostin käytön ja muut luottamuksellisen tiedon jakamisen tavat
- mitä tarkoitetaan henkilötiedoilla ja mitkä ovat omiin työtehtäviin liittyvien henkilötietojen käsittelyn perusteet
- miten kerätä ja käsitellä vain tarkoituksenmukaisia henkilötietoja
- mitä ovat arkaluonteiset henkilötiedot ja kenellä on oikeus käsitellä niitä Laureassa
- mistä löytyvät tietoturvapolitiikka, tietosuojapolitiikka, arkistonmuodostussuunnitelma/ tiedonohjaussuunnitelma ja muut käytännön ohjeet
- miten ottaa epäilyttävissä tai epäselvissä tilanteissa yhteyttä aina ServiceDeskiin tai tehdä turvallisuuspoikkeamailmoitus
- tietosuojavastaavan ja tietoturvavastaavan yhteystiedot.

7 TOIMENPITEET TAVOITETILAAN PÄÄSEMISEKSI

Tiedonhallinnan osaamisen toimintamallia luodessa on ymmärrettävä oman organisaation toimintaympäristö, strategiset tavoitteet sekä henkilöstön tarpeet ja osaamisen taso. (Andreasson ym. 2017, 50.) Osaamisen tukeminen on nähtävä keskusteluprosessina, joka on yksi tärkeimmistä oppimisen edellytyksistä asiantuntijaorganisaatiossa. Vuorovaikutuksen ja kriittisen pohdiskelun avulla synnytetään yhteinen näkemys, jota voi pitää työyhteisön oppimisen ja kehittymisen ydinasiana. (Juholin 2008, 290.) Erityisen tärkeää on osallistaa henkilöstö mukaan niin koulutuksien suunnitteluun, ohjeiden jalkauttamiseen kuin tiedonhallinnan nykytilan kartoitukseen. Osallistavat työmenetelmät edistävät samalla yhteistä sitoutumista, kun tieto ei tunnu ylhäältä päin annetulta.

Osana EU:n yleisen tietosuoja-asetuksen toimenpiteisiin valmistautumista työtä henkilöstön tietosuojaosaamisen vahvistamiseksi tehdään myös muissa Suomen korkeakouluissa. Asiantuntijaosaamista ja hyviä käytänteitä on myös syytä jakaa ja käyttää hyväksi valtakunnallisella tasolla.

7.1 Viestintä lähtökohtana

Laurean strategia 2020:n ja hyvinvointikysely Great Place to Workin tulosten pohjalta on laadittu yhteiset kehittämisalueet Laureassa, joiden otsikkoina on Selkeyttä viestintään ja Minä yhteishengen vaalijana. Nämä teemat on hyvä

pitää esillä myös henkilöstön tiedonhallintaa kehitettäessä, sillä tiedonhallinnan osaamisen kehittäminen kytkeytyy vahvasti molempiin kehittämisalueisiin. Karjalaisen (2011) mukaan selkeällä viestinnällä on tärkein merkitys oikeiden toimintatapojen jalkauttamisessa. Mäkinen (2013) puolestaan toteaa, että yhteisesti sovitut toimintatavat lisäävät niihin sitoutumista ja tätä kautta myös yhteishenkeä. Onkin ensiarvoisen tärkeää viestiä ja ohjeistaa henkilöstöä heidän lähtökohdistaan. Hyvään tiedonhallintaan liittyvän yleisesitteen tekeminen yhteistyössä markkinoinnin kanssa, intra-sivujen päivittäminen, tietoiskujen pitäminen sekä ohjeiden lisääminen Service-Portaaliin on hyvä alku, mutta ne eivät yksinään riitä.

Viestinnän ja ohjeistuksien on oltava myös niin selkeitä, etteivät ne jätä tulkinnan varaa. Ohjeet, kuvaukset ja tekstit ovat sen vuoksi toteutettava paitsi markkinoinnin myös kyseisen toiminnasta vastaavien henkilöiden kanssa, jotta varmistutaan yhteisisistä käsitteistä ja kielestä. Myös viestintäkanavat on syytä luokitella tiedon kriittisyyden ja vaikuttavuuden mukaan. Jos viestit koskettavat koko henkilökuntaa ja niiden noudattamatta jättämisestä johtuvat väärät toimintatavat voivat aiheuttaa vahinkoa, on niiden oltava näkyvästi koko henkilökunnan saatavilla. Prioriteetiltaan tarkeimpiä asioita ovat esimerkiksi akuutit tiedotteet tietoturva-aukkojen päivityksistä tai uhista, jotta käyttäjät tietävät heti, mitä toimia heiltä vaaditaan. Yleiset ohjeet on hyvä koota intraan, josta ne ovat tarvittaessa löydettävissä.

Hyvänä keinona ohjeiden jalkauttamiseen voi toimia myös palvelumuotoilun käyttäjälähtöiset toimenpiteet. Niiden avulla voidaan luoda erilaisia käyttäjäprofiileja perustuen henkilöstön jäsenten käyttäytymismalleihin. Vertailemalla erilaisia henkilökuvauksia voidaan tunnistaa käyttäjäryhmien ominaispiirteitä ja ymmärtää heidän tapaansa toimia tietyissä tilanteissa ja tätä kautta soveltaa ohjeita heidän näkökulmastaan. Reilu viisikymppinen sosiaalialan lehtori omaksuu tietoa hyvin eri tavalla kuin vaikkapa teknisesti suuntautunut kolmekymppinen koulutussuunnittelija.

Lisäksi QPR-järjestelmässä olevat prosessi- ja tietoarkkitehtuurikuvaukset on saatava ajan tasalle, jotta ne voivat ohjata toimintaa. Tulevaisuudessa myös arkistonmuodostussuunnitelma tukee asiakirjojen hallinnan ohjeistusta. Kun se on saatu päivitettyä riittävälle tasolle, on sitä ylläpidettävä intrassa

Osaamistestin perusteella priorisoidaan ensimmäiseksi salatun sähköpostin ja tiedon salassapitoon ja julkisuuteen liittyvät ohjeistukset muun muassa toteuttamalla yleisten ohjeiden lisäksi lyhyet videot, joissa tietoa avataan selkeiden esimerkkien avulla. Osaamistestitulosten mukaisin ”liikennevaloin” voidaan osoittaa samalla henkilöstön osaamisen kehittämiskohteita ja herättää keskustelua siitä, miten henkilöt tällä hetkellä toimivat. Tiedon julkisuuden ja salassapidon osalta on myös syytä avata kuvaa Laurean tietoaineiston käsittelystä konkreettisin esimerkein siitä, miten julkista, käyttörajoitettua ja luottamuksellista tietoa käsitellään niin järjestelmissä kuin järjestelmien ulkopuolella. Samoin henkilötietojen keräämiseen liittyvät menetelmät sekä opiskelijoiden arkaluonteisten tietojen käsittelyyn liittyvät oikeudet ja velvoitteet on ohjeistettava selkeästi.

Tietosuoja- ja tietoturvaohjausryhmän toiminta on oltava myös avointa. Yhtenä ohjausryhmän toimenpiteenä on laatia tietotilinpäätös, jota on hyvä työstää avoimessa intran työtilassa, jotta halukkaat voivat seurata ja kommentoida sitä. Tietotilinpäätöksen avulla voidaan osoittaa kaikki toimenpiteet, joihin Laurea on ryhtynyt hyvän vaaliakseen hyvää tiedonhallintatapaa.

Viestinnän ja ohjeiden hallinta on oltava jatkuva prosessi ja niiden päivittäminen on merkittävä vuosikelloon. Ohjeiden päivittämisen dokumentointi edistää myös EU:n tietosuoja-asetuksen osoitusvelvollisuuden täyttämistä. Pitämällä yllä ajantasaisia ohjeita ja tiedottamalla säännöllisesti, voidaan osoittaa, että henkilöstön osaamisesta pidetään huolta.

7.2 Perehdytys ja koulutus

Perehdyttämiseen kuuluu olennaisena osana organisaation ohjeiden ja määräysten jalkauttaminen. Perehdyttämisestä on myös pidettävä dokumentaatiota. Lisäksi on tärkeää huomioida muutostilanteet, kun henkilö esimerkiksi vaihtaa työtehtäviä tai yksikköä. (Andreasson ym. 2017.)

Osaamisen johtamisen lähtökohdista on tiedonhallinnan osaamisvaatimukset määriteltävä rooleittain. Vähintään perusosaamisen taso on oltava kaikilla Laurean henkilöstön jäsenillä, jotka käsittelevät työssään käyttörajoitettuja tietoa. Lisävaatimuksia osaamiselle on luottamuksellista ja arkaluonteista tietoa

käsittelevillä henkilöillä, joita ovat esimiesten lisäksi henkilöstöhallinnon, talouspalveluiden, tutkimus- ja kehitysyksikön sekä kirjaston henkilökuntaan kuuluvat asiantuntijat sekä tiettyihin opiskelijoiden päätöksiin osallistuvat lehtorit. Kriittistä tietoa käsitteleviin henkilöihin kuuluvat puolestaan turvallisuudesta vastaavat henkilöt ja Laurean johto.

Osaamisvaatimukset on laadittava yhteistyössä HR:n ja turvallisuusjohtajan kanssa ja niiden jalkauttaminen on vastuutettava esimiehille. Tiedonhallinnan osaaminen on kytkettävä vahvasti mukaan myös Digitalisaatio2020-työhön, jolla edistetään laurealaisten digitaitoja. Erityisen tärkeää on varmistaa esimiesten osaamistaso. Koulutusyhteistyötä jatketaan HR:n kanssa tältä osin erikseen.

Osaamisvaatimusten mukaista koulutusta on järjestettävä aluksi koko henkilöstölle, jonka jälkeen koulutus on organisoitava kaikille uusille työntekijöille. Myös yleisiä yksikkö- tai tehtäväroolikohtaisia tietoturva- ja tietosuojainfoja on syytä kalenteroida lukuvuodelle 2017 – 2018. Tämänkin jälkeen infoja on hyvä pitää vähintään parin vuoden välein. Jotta koulutussuunnitelma konkretisoituu, on tehtäväroolien mukaiset koulutukset merkittävä pedakoulutuskalenteriin jo vuodelle 2018.

Yksi osa oikeaa tietoturvallista käyttäytymistä on Karjalaisen (2011) mukaan myös toiminta esimerkin voimalla. Kielloilla ja käskyillä voidaan pahimmillaan aiheuttaa päinvastaista toimintaa, mutta jos kollega vaivihkaa opastaa oikeanlaiseen toimintaan, voi työntekijä ymmärtää paremmin toiminnan tavoitteet. Uusien työntekijöiden osalta tärkeässä roolissa ovat nimetyt lähiohjaajat, joille on luotava oma hyvän tiedonhallinnan perehdyttämisen tarkistuslista. Vanhojen työntekijöiden osalta tietosuoja-agentteina voisivat toimia digimentorit, joita on koulutettu vuosien 2016 ja 2017 aikana yhteensä 14 henkilöä erityisesti kollegoidensa verkko-opetuksen tueksi. Digimentoreiden tehtäviksi on määritelty muun muassa digiosaamisen kasvattaminen omalla kampuksella, digitaalisen toimintakulttuurin muutoksen edistäminen sekä viestintä ja tukipyyntöjen ohjaus tarvittaessa Laurean muihin tukipalveluihin. Digimentoreiden koulutukseen on hyvä lisätä sähköisen tiedon käsittelemiseen, suojaamiseen ja turvaamiseen liittyviä elementtejä, joista he voivat aina sopivan tilaisuuden tullen vinkata kollegoitaan.

Koulutustarpeita voi kartoittaa myös käymällä läpi prosesseja tehtäväryhmittäin prosessien omistajien kanssa Laurean arkistonmuodostus- ja tiedonohjaussuunnitelmatyön ohessa. Tiedonohjauksen avulla mahdollistetaan myöhemmin myös tietojärjestelmissä toteutettava asiakirjatietojen hallinnan automaattinen ohjaus (JUHTA 2016). Yksittäisten esimerkkien ja henkilöstön omien kokemusten kautta voidaan samalla laatia konkreettisia ohjeistuksia erilaisiin tilanteisiin, joihin kaivataan tukea. Prosessin vaiheittain voidaan kuvata, mitä tietoa pitää olla saatavissa, ketkä tietoa tarvitsevat ja miten tietoa hyödynnetään ja käsitellään. Lisäksi voidaan selvittää sitä, tuleeko prosessien hoitamiseen tarvittava tieto ihmisten hiljaisen tiedon avulla vai olemassa olevista ohjeista ja tietojärjestelmistä, jolloin voidaan puuttua virheellisiin tai ylimääräistä työtä aiheuttaviin toimintatapoihin. Samalla voidaan seuloa ja arvioida kaikki yksiköiden keskeisimmät toimintaohjeet. Työn avulla voidaan tunnistaa ne osa-alueet, joiden tiedonhallinnan osaaminen vaatii tehostamista. Samalla voidaan myös huomata, mitä prosessin vaiheita tai kokonaisia prosesseja pitää luoda tai poistaa kokonaan esimerkiksi tiedon automatisoinnin avulla. (Linden 2015.) Tällä tuetaan sekä laurealaista osaamista että digivisiota.

Lisäksi prosesseissa käsiteltävien tietojen kartoitus tukee myös henkilötietojen suojaa. Sen avulla voidaan tunnistaa henkilötietojen käsittelijät, käsittelytarkoitukset, integraatiot muihin järjestelmiin sekä henkilötietojen siirtoon ja luovutuksiin liittyvät käytännöt. Samoin voidaan puuttua henkilötietojen keräämisessä muodostuviin henkilörekistereihin, tarvittaviin rekisteriselosteisiin ja ylipäätään tietojen keräämisen oikeuteen. Tässä yhteydessä voi hyvin huomioida myös salassa pidettävän ja arkaluonteisen tiedon käsittelyn vastuut ja riskit.

Prosessien läpikäynnin yhteydessä voidaan kartoittaa myös toimintatapoja, joiden eteen on rakennettava tiedon välittämisen portti, jonka edessä on tietosuojaan liittyviin kysymyksiin koulutettu henkilö. Näin vältytään tiedon mahdolliselta väärinkäytöltä. Julkistakaan tietoa ei ole välttämätöntä heti antaa eteenpäin, vaan koulutettu henkilö voi esimerkiksi tarkastaa, onko kysyjällä oikeus tiedon saamiseen ja onko syytä epäillä, että tietoa käytetään muuhun tarkoitukseen kuin pyydettyyn. Erityisesti opintohallinnosta on voi antaa vastuun yh-

delle koulutetulle henkilölle, jolla on tarvittava opintohallinnon prosessien ajantasainen tieto tietosuojaan liittyen. Näin kaikkien opintosihteereiden ei tarvitse olla huolissaan siitä, toimiiko oikein tiedon antamiseen ja luovuttamiseen liittyvissä kysymyksissä.

7.3 Osaamisen mittaaminen ja seuranta

Pirjo Jokelainen (2011) toteaa pro gradu –työssään, että tietoturva- ja tietosuojaosaamista voidaan mitata useasta eri näkökulmasta. Mitattavina kohteina voivat olla muun muassa opitut tiedot ja taidot, soveltaminen, asenteet ja arvot sekä henkilökohtaisen suorituskyvyn kehittyminen. Jos lasketaan ainoastaan koulutusten osallistumismääriä, ei saada tietoa todellisesta osaamisen tasosta. Teoriaosaamisia voidaan testata muun muassa näyttökokeilla tai itsearvioinneilla tai esimiehen tekemän arvioinnin pohjalta.

Koulutusten ja ohjeistusten ohella tiedonhallinnan osaamistesti toimii Laureassa jatkossa sekä henkilöstön perehdyttämisen seurannan, että osaamistason mittaamisen välineenä. Tavoitteena on tehdä testi myös sähköiseen muotoon, johon henkilöstö voi vastailla osana perehdytystä ja pedakoulutusta. Sähköisen kyselyn avulla saadaan kerättyä dataa henkilöstön osaamistason karttumisesta. Tuloksia on hyvä käydä läpi myös kehityskeskusteluissa, jotta koulutusta voidaan kohdentaa myös henkilötasolla tarvittaviin osa-alueisiin. Testi on hyvä toteuttaa kolmiportaisena tehtävärooleittain, jossa ensimmäinen taso mittaa perusosaamista. Seuraava tason on suoritettava, jos käsittelee työssään luottamuksellista tietoa. Kolmas taso on tarkoitettu johdolle ja turvallisuudesta vastaaville henkilöille, joilla on oltava kattavin tietosuojan ja tietoturvan osaamisen taso.

Tietosuoja- ja tietoturvaohjausryhmän tehtävä on päättää ne mittarit, millä henkilöstön osaamista mitataan. Tunnuslukujen kerääminen on tärkeää, jotta voidaan varautua mahdollisiin riskeihin ja huomata mahdolliset pinnalle nousevat asiat. Ehdotuksia mitattaviksi luvuiksi ovat

- Tietosuoja- ja tietoturvapoikkeamailmoitusten määrä
- Henkilöstön koulutuspäivät
- Salatun sähköpostin tilastot
- Osaamistestin tulokset

- Tietosuoja- ja tietoturvavastaavalle osoitettujen kyselyiden määrä ja aiheet
- Hyvinvointikyselyn tulokset erityisesti liittyen saatuun tukeen liittyen

7.4 Tulevaisuuden haasteita

Osaamistestin tulokset osoittavat, että Laurean lukuiset tiedontallennuspaikat eivät tule sähköistä asiakirjanhallintaa ja sähköistä arkistointia ja että Laureassa on tarve asiakirjojen hallintajärjestelmälle ja sähköiselle arkistolle. Mahdollisen asianhallintajärjestelmän hankinta on kuitenkin pohjauduttava vahvasti henkilöstön tarpeisiin ja vaatimuksiin, sillä se muuttaa aina organisaation toimintaa ja prosesseja. Sen vuoksi järjestelmähankinta on erityisen kriittinen vaihe, jotta sitä voidaan hyödyntää tehokkaalla tavalla eikä se jää vajaakäytölle. Jo määrittelyvaiheessa on huomioitava Karjalaisen (2011) tutkimuksen mukaisesti, että jokaisella työntekijällä on omanlaisensa kyky, halu ja osaaminen tiedon omaksumisen tapoihin, mikä vaikuttaa myös järjestelmän käyttämisen motivaatioon ja uusien toimintatapojen oppimiseen (Linden 2015). Henttonen (2015) muistuttaa myös, että henkilöstä ei voi suoraan pakottaa käyttämään tiedonhallintajärjestelmiä, mutta niitä voidaan lähteä edistämään ratkaisuna oman työn parempaan tiedonhallintaan. Tämän vuoksi on hyvä yhteisesti pohtia keinoja, joilla omien dokumenttien ja muiden tietojen systemaattisella tallentamisella yhteiseen järjestelmään ei vain paranna omaa työhyvinvointiaan vaan myös auttaa kollegoiden tiedonhallintaa.

Uusia haasteita tuovat myös lainsäädännön uudistuminen. Tietoturva- ja tietosuojaohjausryhmän on seurattava EU:n tietosuoja-asetuksen lisäksi tiedonhallintalain ja tietosuojalain valmistelua samoin kuin valtakunnallisissa työryhmissä ja yleisesti julkisuudessa käytävää keskustelua. Tältä pohjalta on määriteltävä uusia digitalisen tiedonhallinnan vaatimuksia henkilöstön osaamiselle. Lainsäädännön ja digitaalisten toimintatapojen kehitystä on käytävä läpi säännöllisesti niin tietosuoja- tietoturvaohjausryhmän palavereissa kuin Laurean Digitalisaatio2020 -työssä ja luonnollisesti niiden aiheuttamista toimenpiteistä on raportoitava myös johdolle.

8 POHDINTA

Kun kevättalven 2017 kehityskeskustelussani lupauduin ottamaan Laurean tietosuojavastaavan tehtävät vastaan, en vielä osannut aavistakaan, millainen tehtäväkenttä minulla olisi edessä. Osana YAMK-opintojani olin toki hieman käynyt jo läpi henkilötietojen käsittelyyn liittyviä asioita, mutta rehellisesti sanottuna lähes kaikki oli minulle ihan uutta. Kävin Lakimiesliiton tietosuojavastaavan koulutuksen ja luin tietosuojaan liittyviä kirjoja, artikkeleita ja verkkosivuja. Opettelin ulkoa EU:n tietosuoja-asetuksen vaatimuksia, pohdin mielessäni, mitä eroa on salassa pidettävällä, salaisella ja luottamuksellisella tiedolla ja yritin jäsentää kaikkia toimenpiteitä, joihin Laureassa on ryhdyttävä ennen tietosuoja-asetuksen soveltamisen voimaantuloa. Samalla pohdin, miten voisin kytkeä aiheen opinnäytetyöhöni.

Paitsi että tietosuojavastaavan on seurattava voimassaolevan lainsäädännön noudattamista, on yksi tietosuojavastaavan tärkeimmistä tehtävistä myös kouluttaa ja ohjeistaa henkilöstöä. Henkilöstön tiedonhallinnan osaamisen kehittäminen muodostui siten sekä omaa työtäni että osaamistani tukevaksi opinnäytetyön aiheeksi. Työ henkilöstön osaamisen hallinnan parissa on ollut myös omanlaisensa kasvun paikka. Olen joutunut haastamaan itseäni ja ottamaan paikkani asiantuntijaorganisaatiossa. Ymmärtämään sen, että tieto ei välttämättä lisää toivottua käyttäytymistä ja asennetta, ellei sitä osata tarjota oikein. Ymmärtämään, että yhteistyöllä saa enemmän aikaan kuin käskyttämällä.

Opinnäytetyöni tavoitteena oli selvittää millä tavalla ammattikorkeakoulun nykyiset toimintamallit tukevat henkilöstön hyvän tiedonhallintatavan omaksumista. Selvityksen perusteella Laurean nykyiset toimintamallit eivät edistä riittävällä tasolla hyvää tiedonhallintaa. Ohjeita on niukalti ja osa niistä on päivittämättä. Tietosuojaa ja tietoturvaa ei ole otettu riittävällä tasolla mukaan perehdytysohjelmaan eikä siihen ole tarjottu koulutusmahdollisuuksia. Erityisen kriittinen tilanne on esimiesten osalta. Myös heidän on ymmärrettävä, että tiedonhallintaosaaminen ei ole erillinen kokonaisuutensa, vaan se kytkeytyy tärkeäksi osaksi digiajan taitoja.

Henkilöstöpäivillä suoritetun osaamistestin tulokset toimivat tutkimusmateriaalina henkilöstön osaamisen mittaamiselle. Sen mukaan henkilöstö on omaksunut hyvin laajalla skaalalla tietosuojaan ja tietoturvaan liittyvät kysymykset ja 90 % henkilöstöstä kokee, että heillä ei ole tarpeeksi osaamista tietosuojaan ja tietoturvaan liittyvissä asioissa. Lähes kaikilla kysytyillä osa-alueilla oli haasteita, mutta erityisesti tietojen julkisuus ja salassapito sekä luottamuksellisen tiedon jakamisen tavat ovat asioita, jotka nousivat osaamistestissä esiin. On kuitenkin otettava huomioon, että otos edusti vain noin 20 % henkilöstöstä, eikä tuloksista voi tehdä tehtäväkohtaisia johtopäätöksiä henkilöstön osaamisen tasosta. Lisäksi kysymyspatteristo käsitti vain kymmenen tietosuojaan ja tietoturvaan liittyvää kysymystä, joten osaamistasoa voi mitata vain näiden kysymysten tai väitteiden osalta. Osaamistestin tuloksiin saattoivat vaikuttaa osin myös moniselitteiset kysymykset ja käsitteet. Toisaalta tämä kertoo siitä, että juuri käsitteiden, kuten henkilötiedon, salassa pidettävän ja asiakirjallisen tiedon määritteleminen auttaisi henkilöstöä omaksumaan tiedonhallintaa yhä paremmin. Osaamistestin tulosten ”liikennevaloja” kannattaa kuitenkin käyttää hyväkseen nyt mahdollisimman paljon niin keskustelun herättäjänä, viestinnässä kuin koulutusten suunnittelussa.

Jotta tietojen julkisuuteen, käsittelemiseen, suojaamiseen ja turvaamiseen liittyvät tiedot tulevat koko henkilöstön saataville on Laurean ymmärrettävä henkilöstön osaamistasoon, käyttäytymiseen ja asenteisiin vaikuttavat seikat niin henkilöiden aiempien kokemusten kuin omien henkilökohtaisten ominaisuuksiensa kautta. 500 työntekijän asiantuntijaorganisaatio muodostuu 500 erilaisesta persoonasta, joilla jokaisella on omanlaisensa kokemus tietojärjestelmistä ja omat henkilökohtaiset ominaisuutensa. Asiantuntijaorganisaatiossa asenteisiin vaikuttaminen voikin olla yksi suurimmista haasteista. Palvelumuotoilun avulla henkilöiden tarpeita voidaan kuitenkin profiloida, ja tehdä ohjeet heitä parhaiten palveleviksi.

Teemahaastatteluissa nousi esiin myös perehdytyksen tarve ja erityisesti arkaluonteisen tiedon käsittelyn kysymykset. Nämä ovat selkeitä kehityskohteita, jotka ovat erityisesti HR:n ja turvallisuusjohtajan vastuulla. Hyvään tiedonhallintaan liittyvällä tietojenkäsittelyllä on oltava yhä merkittävämpi osa perehdyttämistä, esimiesten työn tukemista unohtamatta. Toisaalta myös koko

henkilöstön on omaksuttava tarvittavat käsitteet ja mahdolliset uudet toimintamallit uudenlaisten tiedonhallintaratkaisujen puitteissa. Tätä työtä tukee muun muassa tiedonohjaussuunnitelmatyö sekä mahdollinen asianhallintajärjestelmän käyttöönotto, johon on osallistettava vähintään kaikki prosessien omistajat. Prosessien läpikäynti on kuitenkin oma erillinen projektoitava tehtäväkokonaisuutensa, joka tulee viemään aikaa kuukausia ellei vuosia. Tiedonohjaussuunnitelmatyö ja järjestelmähankinta voivat myös omalta osaltaan vaikuttaa tiedonhallinnan osaamiseen, vaikka eivät varsinaisesti ole osa tiedonhallinnan osaamisen kehittämistä.

Koska opinnäytetyöni on tässä vaiheessa vasta suunnitelma osaamisen vahvistamiseksi, jää tulosten seuraaminen seuraavan selvityksen aiheeksi. Tärkeä osa osaamisen seurantaa onkin sen mittaaminen. Mittareista ei kuitenkaan ole hyötyä, jos ne eivät mittaa oikeita asioita tai niitä ei seurata. Mittareiden arviointityössä on tietosuoja- ja tietoturvaohjausryhmällä merkittävä rooli. Sen on määriteltävä toimintaansa myös tulevaisuuden osaamista silmällä pitäen ja pyrittävä ohjaamaan Laurean toimintaa kohti hyvää tiedonhallintaa, myös tulevaisuudessa, josta vielä emme tiedä mitään. Oman haasteensa työhön tuovat vielä lainsäädännön uudistukset, joiden voimaantuloa vielä odotellaan. Uudistuva lainsäädäntö tuo kuitenkin toivottavasti helpotusta osin vanhentuneita toimintamalleja tukevaan ja vaikeasti tulkittavaan sääntelyyn.

Jatkotutkimuksena olisi kiinnostavaa tutkia, minkälaisia hyötyjä palvelumuotoilun avulla ja henkilöstön eri käyttäjäprofiileja määrittelemällä saadaan osaamisen tukemiseen ja ohjeiden jalkauttamiseen. Toinen tärkeä selvityksen aihe olisi arkaluonteisen tiedon käsittelyn tapojen kartoitus, niiden huomioiminen ja ohjeistuksen vaikutus ammattikorkeakoulun toimintaan.

Yhä tuntuu, että mitä enemmän olen opiskellut tietoturvaan ja tietosuojaan liittyneitä asioita, sitä enemmän minulla on vielä opittavaa. Hyvä tiedonhallinnan osaaminen ei koostu kuitenkaan pelkästä ulkoa opetellusta tiedosta, vaan sen on näyttävä myös omassa toiminnassa ja asenteissa, toimimisena esimerkkinä muille. Laurea-ammattikorkeakoulun henkilöstölle puolestani toivon, että he ymmärtäisivät tiedon arvon arkityössään, omaksuisivat itselleen riittävän tiedonhallinnan tason osana digitaitoja ja tuntisivat näin olonsa turvalliseksi omissa toimintatavoissaan.

LÄHTEET

Aholainen, E. 2017. Sisällönhallinta suomalaisessa julkishallinnossa. Tampereen yliopisto. Viestintätietieteiden tiedekunta. Pro gradu -tutkielma.

Ammattikorkeakoululaki 14.11.2014/932.

Andreasson, A. Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Tallinna: Printon.

Arkistolaitoksen arkistowiki 2013. Informaatio. WWW-dokumentti. Päivitetty 24.6.2013. Saatavissa: http://wiki.narc.fi/arkistowiki/index.php/Informaatio. [Viitattu 9.4.2017].

Hakkarainen-Kiri, A. 2014. Kokonaisarkkitehtuuri ja informaation audit – analyysi tiedonhallinnan näkökulmasta. Tampereen yliopisto. Informaatiotieteiden yksikkö. Pro gradu –tutkielma.

Henttonen, P. 2015. Johdatus asiakirjahallinnan tutkimukseen. Vantaa: Hansaprint.

Jokelainen, P. 2011. Hoitohenkilöstön tietoturva- ja tietosuojatietämys. Itä-Suomen yliopisto. Sosiaali- ja terveysjohtamisen laitos. Pro gradu -tutkielma.

Juholin, E. 2008. Viestinnän vallankumous, Löydä uusi työyhteisöviestintä. Porvoo: Bookwell Oy.

JUHTA Julkisen hallinnon tietohallinnon neuvottelukunta 2015. JHS 179. Kokonaisarkkitehtuurityön suunnittelu ja kehittäminen. Liite 9. Tiedonhallinta ja tietoarkkitehtuurityö. PDF-dokumentti. Saatavissa: http://www.jhs-suositukset.fi/c/document_library/get_file?uuid=41df9f7f-27f9-44ac-811a-fbe45961aeae&groupId=14. [Viitattu 10.4.2017].

JUHTA Julkisen hallinnon tietohallinnon neuvottelukunta. 2016. JHS 191. Tiedonohjaussuunnitelman rakenne. PDF-dokumentti. Saatavissa: http://www.jhs-suositukset.fi/suomi/jhs191. [Viitattu 1.9.2017].

Karjalainen, M. 2011. Improving employees' information systems (IS) security behavior: toward a meta-theory of IS security training and a new framework for understanding employees' IS security behavior. Oulun yliopisto. Luonnontieteellinen tiedekunta. Väitöskirja.

Karppinen, L, Johansson, A. 2017. Korkeakoulujen opintotietojen tietosuojan käytännesäännöt. PDF-dokumentti. Saatavissa: https://wiki.eduuni.fi/display/CSCKOOTUKI/Korkeakoulujen+opintotietojen+tietosuojan+kaytannesaannot [Viitattu 20.9.2017].

Korkeakoulujen KA-Pilotti ryhmä 2013. KARTTURI. Korkeakoulujen kokonaisarkkitehtuuri menetelmäopas. Päivitetty 13.8.2013. Saatavissa: https://confluence.csc.fi/display/RAKETTI/Kartturi. [Viitattu 10.4.2017].

Kruger, H, Kearney, A. 2006. A prototype for assessing information security awareness. Computers & Security 25/2006, 289-296.

Laki julkisen hallinnon tietohallinnon ohjauksesta. 10.6.2011/634.

Laki viranomaisen toiminnan julkisuudesta. 21.5.1999/621.

Laurea-ammattikorkeakoulu 2016. Strategia 2020. PDF-dokumentti. Saatavissa: http://markkinointi.laurea.fi/strategia2020/. [Viitattu 29.9.2017].

Laurea-ammattikorkeakoulu 2017. Vuosikatsaus 2016. PDF-dokumentti. Saatavissa: https://indd.adobe.com/view/c9cf7aa4-c60c-4183-b651-bc68fe54f29b. [Viitattu 29.9.2017].

Linden, J. 2015. Tiedonhallinta & yrityksen menestys. Tampere: Juvenes Print.

Mäkinen, S. 2013. Records Management in Mobile Work. Tampereen yliopisto. Informaatiotutkimuksen ja interaktiivisen median laitos. Väitöskirja.

Oikeusministeriö 2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö. 35/2017.

Puolustusministeriö 2011. Kansallinen turvallisuusauditointikriteeristö. PDF-dokumentti. Saatavissa: http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf. [Viitattu 2.10.2017].

Suomen standardisoimisliitto 2017. Tietoturvatekniikat. WWW-dokumentti. Saatavissa: https://www.sfs.fi/standardien_laadinta/sfs_n_tekniset_komiteat_ja_seurantaryhmat/it-standardisointi/it_-_aihealueet/tietoturvatekniikat. [Viitattu 17.10.2017].

Tietosuojavaltuutetun toimisto 2012. Laadi tietotilinpäätös. PDF-dokumentti. Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf. [Viitattu 2.10.2017].

Tietosuojavaltuutetun toimisto 2010. Ota oppaaksi henkilötietolaki! PDF-dokumentti. Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq7xbJn/Ota_oppaaksi_henkilotietolaki_teksti.pdf. [Viitattu 1.10.2017].

Tietosuojavaltuutetun toimisto 2014. Rekisteröityjen oikeudet. WWW-dokumentti. Saatavissa: http://www.tietosuoja.fi/fi/index/rekisteroidylle/rekisteroidynoikeudet.html. [Viitattu 28.9.2017].

Tietosuojavaltuutetun toimisto 2016. Kysymyksiä ja vastauksia tietosuojauudistuksesta. WWW-dokumentti. Saatavissa: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html. [Viitattu 28.9.2017].

Tietoyhteiskuntakaari 7.11.2014/917.

Valtioneuvosto 2010. Valtioneuvoston asetus tietoturvallisuudesta. 681/2010.

Valtiovarainministeriö 2010. Hyvä tiedonhallinta- ja käsittelytapa. WWW-dokumentti. Päivitetty 29.10.2010. Saatavissa: https://www.vahtiohje.fi/web/guest/hyva-tiedonhallinta-ja-tiedonkasittelytapa. [Viitattu 10.9.2017].

Valtiovarainministeriö 2010. Tietoaineiston luokittelu. Vahti-ohje. WWW-dokumentti. Saatavissa: https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu. [Viitattu 13.10.2017].

Valtiovarainministeriö 2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti 1/2016. PDF-dokumentti. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229. [Viitattu 1.9.2017].

Valtiovarainministeriö 2017a. Julkisen hallinnon kokonaisarkkitehtuuri Tiedonhallinnan prosessit ja tietoarkkitehtuurin suunnittelu. PDF-dokumentti. Saatavissa: https://wiki.julkict.fi/. [Viitattu 29.9.2017].

Valtiovarainministeriö 2017b. Tiedonhallinnan lainsäädännön kehittämislinjaukset. Valtiovarainministeriön julkaisu 37/2017. PDF-dokumentti. Saatavissa: http://vnk.fi/documents/10623/306884/37_2017_Tiedonhallinnan+lains%C3%A4%C3%A4d%C3%A4nn%C3%B6n+kehitt%C3%A4mislinjaukset.pdf/c1f679f5-a26b-4308-9162-c395b3f5d093. [Viitattu 22.10.2017].

Vilkka, H. 2015. Tutki ja kehitä. Jyväskylä: PS-kustannus.

Vilminko-Heikkinen, R. 2017. Data, Technology and People – Demystifying Master Data Management. Tampereen yliopisto. Talouden ja rakentamisen tiedekunta. Väitöskirja.

Voutilainen, T. 2012. Oikeus tietoon. Informaatio-oikeuden perusteet. Porvoo: Bookwell oy.

Voutilainen, T. 2014. Julkisen hallinnon pirstaloituneisuus tiedonhallinnan ongelmana. Teoksessa Jääskeläinen A. (toim.) Digitaalisuus tässä ja nyt. Osaammeko luopua vanhasta? Mikkeli: Tammerprint, 9-16.

TIETOSUOJA JA TIETOTURVA LAUREASSA

Tiedon suojaaminen ja turvaaminen ovat oleellinen osa toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja päivittäistä tietojen käsittelyä.

Tietosuojan ja tietoturvallisuuden hyvä hallinta edellyttävät tietojen käsittelyn jatkuvaa seurantaa, pitkäjänteistä suunnittelua, erilaisiin uhkatilanteisiin varautumista, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää.

Tietosuojan ja tietoturvan toteuttaminen on jatkuvaa ja laaja-alaista toimintaa, jota ei voida asettaa vain muutaman vastuuhenkilön tai tekniikan vastuulle. Tarvitsemme tiivistä ja rakentavaa yhteistyötä kaikkien yhteisöömme kuuluvien henkilöiden ja ryhmien kesken.

Erityisen tärkeää on tiedostaa oman toiminnan merkitys omaan ja muiden tietoturvaan ja henkilötietojen suojaamiseen.

Vastaa oheisiin kysymyksiin ja testaa osaamisesi ja toimintatapasi!

Mitä ajatuksia testi herätti?

Mitkä seuraavista ovat luottamuksellisia tai salassa pidettäviä tietoja?	
	Kaikki yksittäiset henkilötiedot
	Päätös opiskelijan erityisen tuen järjestelyistä
	Opiskelijan koesuoritus
	Päätös opiskelijan lisäaikahakemukseen
	Opiskelijanumero
	Kaikki terveyteen liittyvä tieto
	Henkilötunnus
Tällä hetkellä säilytän luottamuksellisia dokumenttejani	
	Tulostettuna käsieni ulottuvilla työpöydälläni
	Oman tietokoneen kovalevyllä
	Verkkolevyn H-asemalla
	Kotona
	Muualla, missä?
Jos minun on jaettava työasioissa luottamuksellista tietoa, teen sen yleensä	
	Sähköpostitse
	Pilvipalvelussa (esim. Google Drive)
	Intranetin työtilassa
	Skypellä
	Salatulla sähköpostilla
	Muulla tavalla, millä?

Jos huomaan pääseväni käsiksi minulle kuulumattomiin toista henkilöä koskeviin luottamuksellisiin tietoihin, toimin seuraavasti	
	Pyrin olemaan asiasta mahdollisimman hiljaa
	Käyn tiedot läpi mahdollisimman tarkkaan, jotta tiedän varmasti kuka niistä vastaa
	Tuhoan tiedot välittömästi
	Teen asiasta turvallisuuspoikkeamailmoituksen
	Ilmoitan asiasta ko. henkilölle
Voin lähtökohtaisesti kertoa kysyjälle seuraavista asioista	
	Kollegan sairauslomasta
	Opiskelijan tenttituloksesta
	Opiskeleeko jokin tietty henkilö Laureassa
	Opiskelijan kotiosoitteen
	Kollegan puhelinnumeron
	Onko opiskelija saanut kirjallisen varoituksen
Käytän salattua sähköpostia seuraavissa tapauksissa	
	Kun lähetän viestin Laurean ulkopuolelle
	Aina kun viesti sisältää henkilötietoja
	Kun viestissä on jonkun henkilön henkilötunnus
	Kun lähetän sairauslomatodistukseni esimiehelleni
	En koskaan
	En tiedä, mikä on salattu sähköposti

Kun epäilen saaneeni haitallisen sähköpostiviestin, toimin seuraavasti	
	Katson intrasta, onko vastaavista viesteistä tiedotettu Laureassa
	Soitan ServiceDeskiin
	Poistan viestin välittömästi
	Katson, mitä viestin liite sisältää, ja toimin tarvittaessa vasta sitten
	Jätän viestin omaan arvoonsa
Järjestän tapahtumaa, johon olen kerännyt osallistujien sähköpostiosoitteet kontaktointia varten. Tapahtuman lähestyessä haluan lähettää osallistujille tervetuloviestin. Miten toimin?	
	Lähetän jokaiselle osallistujalle erikseen oman viestin
	Lähetän viestin piilokopiona osallistujille
	Kirjoitan osallistujien sähköpostiosoitteet vastaanottajakenttään ja lähetän viestin kaikille
	Lähetän viestin salattuna sähköpostina
Säilytän opiskelijoiden tekemiä oppimistehtäviä ja tenttejä	
	Yli 5 vuotta
	Yli vuoden mutta alle 5 vuotta
	Noin vuoden verran
	6 kuukautta
	Tuhoan heti, kun arvosanat on kirjattu

Minulla on oikeus	
	kieltää Laureaa antamasta minua koskevia tietoja tarvittaessa viranomaisille
	pyytää nähtäväksi kaikki Laureassa minusta kerätyt tiedot
	vaatia virheellisen tai vanhentuneen tietoni korjaamista
	kieltää tietojeni käyttöä markkinatutkimusta varten
	vaatia kaikkien tietojeni poistamista Laurean järjestelmistä lähtiessäni pois Laureasta

Mistä haluaisin lisätietoa, mikä jäi vielä askarruttamaan…?

Liite 2

KUVALUETTELO